



User Guide for the Cisco Mobile Wireless Transport Manager 6.1

November 2008

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-13314-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

User Guide for the Cisco Mobile Wireless Transport Manager 6.1
Copyright © 2005-2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

About This Guide xxxi

CHAPTER 1

Overview 1-1

- What Is the MWTM? 1-1
 - Server and Network Features 1-2
 - Graphical User Interface and Web Features 1-2
 - Event Monitoring Features 1-3
 - Performance Features 1-3
 - Provisioning Features 1-3
 - Security Features 1-4
 - Topology Features 1-4
 - Troubleshooting Features 1-4
 - Customization Features 1-5
 - Integration Features 1-5
- What Is ITP? 1-6
- What is CDT? 1-7
- What is IPRAN? 1-7
- What is PWE3? 1-8
- What Is RAN-O? 1-8
- What Is mSEF? 1-9
- How Do I Identify My Network Type? 1-9
- What Is Client/Server Architecture? 1-10

CHAPTER 2

Configuring Security 2-1

- Configuring User Access 2-1
 - Implementing Secure User Access (Server Only) 2-2
 - Security Authentication 2-2
 - User Levels 2-4
 - User Passwords 2-4
 - Enabling Secure User Access 2-6
 - Creating Secure Passwords 2-7
 - Configuring MWTM User Account Levels (Server Only) 2-7
 - Basic User (Level 1) Access 2-8
 - Power User (Level 2) Access 2-8

Network Operator (Level 3) Access	2-9
Network Administrator (Level 4) Access	2-9
System Administrator (Level 5) Access	2-11
Automatically Disabling Users and Passwords (Server Only)	2-11
Manually Disabling Users and Passwords (Server Only)	2-13
Enabling and Changing Users and Passwords (Server Only)	2-14
Displaying a Message of the Day (Server Only)	2-16
Manually Synchronizing Local MWTM Passwords (Server Only)	2-17
Listing All Currently Defined Users (Server Only)	2-18
Displaying the Contents of the System Security Log (Server Only)	2-18
Restoring Security-Related MWTM Data (Server Only)	2-19
Disabling MWTM User-Based Access (Server Only)	2-20
Specifying a Super User (Server Only)	2-20
Implementing SSL Support in the MWTM	2-22
Enabling SSL Support on the MWTM Server	2-22
Downloading the MWTM SSL Module for Windows Using the Web Interface	2-24
Downloading the Self-Signed SSL Certificate from the MWTM Server	2-26
Launching the MWTM Certificate Tool for SSL	2-26
Importing an SSL Certificate to an MWTM Client	2-27
Exporting an SSL Certificate	2-28
Viewing Detailed Information About a SSL Certificate	2-29
Managing SSL Support in the MWTM	2-30
Disabling SSL Support in the MWTM	2-30
Limiting MWTM Client Access to the MWTM Server (Server Only)	2-31
Backing Up or Restoring MWTM Files (Server Only)	2-32
Backing Up MWTM Data Files	2-32
Changing the Backup Directory	2-33
Setting the Number of Backup Days	2-33
Restoring the MWTM Data Files	2-34
Removing MWTM Data from the MWTM Server	2-35

CHAPTER 3

Setting Up Your Server 3-1

Importing SNMP Community Names from CiscoWorks (Solaris Only)	3-2
Changing MWTM Server Poller Settings	3-2
Changing the Message Display	3-4
Changing the Location of MWTM Message Log Files	3-4
Changing the Size of the MWTM Message Log Files	3-4
Changing the Time Mode for Dates in Log Files	3-5
Changing the Age of the MWTM Message Log Files	3-5

Setting the ITP Point Code Format	3-5
Connecting a Single-Instance ITP to a Multiple-Instance ITP	3-6
Enabling SNMP Traps	3-7
Limiting Traps by IP Address	3-9
Configuring a Backup MWTM Server	3-10
Configuring an MWTM Client Connection Timer	3-11
Enabling the Terminal Server Proxy Service	3-11
Setting Up TFTP on Your Server (ITP Only)	3-12
Setting Up TFTP on Solaris	3-12
Setting Up TFTP on Linux	3-13
Configuring Nodes	3-14
Node SNMP and Credentials Menu	3-15
Configuring SNMP Settings	3-15
SNMP Settings Table	3-16
SNMP Configuration Table	3-16
SNMP Configuration Buttons	3-18
SNMP Configuration Commands	3-18
Configuring Login Credentials	3-20
Setting Up Login Credentials	3-20
Credentials Fields	3-21
Credentials Buttons	3-22
Adding Nodes	3-23
Credentials Commands	3-23
Creating New Troubleshooting Categories and Commands	3-23

CHAPTER 4

Getting Started 4-1

Starting the MWTM Server	4-1
Becoming the Root User (Server Only)	4-2
Starting the MWTM Client	4-2
Before Starting the MWTM Client	4-3
Setting the DISPLAY Variable for Solaris or Linux Clients	4-3
Starting the MWTM Client on Solaris or Linux	4-3
Access the Node	4-4
Starting the MWTM Client on Windows	4-4
Discovering Your Network	4-4
Discovery Overview	4-4
Launching the Discovery Dialog	4-6
Discovery Dialog Menu	4-6

Discovery Dialog Tabs	4-6
Loading Seed Nodes and Seed Files	4-7
Loading a Seed Node	4-7
Loading a Seed File	4-7
Saving a Seed File	4-8
Creating a New Seed File	4-10
Changing an Existing Seed File	4-11
Creating and Changing Seed Files Using a Text Editor	4-12
Running Discovery	4-12
Discovery Settings	4-13
Discovered Nodes	4-15
Verifying Discovery	4-15
Displaying the MWTM Main Window	4-16
Navigational Features	4-17
MWTM Client Navigation Tree	4-19
MWTM Client Content Area	4-19
Displaying Summary Lists Alarms	4-19
Right-Click Menu for the Summary Lists	4-20
Using the MWTM Main Menu	4-21
Using the MWTM Toolbar	4-27
Accessing the MWTM Through a Web Browser	4-28
Loading and Saving MWTM Files	4-29
Using the Windows Start Menu	4-30
Changing the Default MWTM Server Name	4-31
Launching the MWTM Client	4-31
Launching the MWTM DOS Prompt	4-31
Launching the MWTM Event Editor	4-31
Launching the MWTM SSL Certificate Tool	4-32
Displaying the MWTM README File	4-32
Uninstalling the MWTM	4-32
Exiting the MWTM Client	4-32

CHAPTER 5

Basic Operations 5-1

Changing Client and Web Preference Settings	5-1
Changing Client Preference Settings	5-2
Displaying the Preferences Menu	5-3
Changing General GUI Settings	5-4
Changing Alarm and Event Settings	5-8
Changing Charts Settings	5-11

Changing Status Settings	5-12
Changing CiscoWorks Server Settings	5-13
Changing Topology Settings	5-14
Changing Deploy Settings	5-16
Customizing Colors	5-18
Restoring Default Preference Settings	5-19
Changing Web Preference Settings	5-20
Changing Real-Time Poller and Counter Settings	5-21
Viewing Online Help	5-22
Finding Information in a Window	5-23
Navigating Table Columns	5-24
Printing Windows	5-25
Managing and Deploying ITP Files	5-25
Node File Management	5-26
Node File Management Menu	5-27
Node File Management MWTM Pane	5-30
Node File Management Node Pane	5-31
Node Archive Management	5-33
Node Archive Management Menu	5-34
Node Archive Management Selector Pane	5-34
Node Archive Management Display Pane	5-35
Deploying ITP Files	5-36
Exporting Data	5-38
Exporting Current Data for Network Objects	5-38
Exporting Current Node Names and SNMP Community Names	5-39
Integrating the MWTM with Other Products	5-39
Integrating the MWTM with CiscoWorks	5-39
Launch CiscoWorks Applications from the MWTM Client	5-40
Launch Integrated Applications from the MWTM Web Interface	5-41
Launch the MWTM Web Interface from the CiscoWorks Dashboard	5-42
Forwarding Traps to Other Hosts (Server Only)	5-42
Running Simultaneous Client Sessions	5-43
Performing Basic Server Operations	5-43
Connecting to a New Server	5-43
Viewing Server Status Information	5-44
Server Status Information: Fields and Buttons	5-44
Server Status Information: Processes	5-45
Server Status Information: Pollers	5-45
Server Status Information: Tasks	5-46

Server Status Information: Clients	5-46
Using the Command Line Interface	5-47

CHAPTER 6

Understanding Basic Object Functions 6-1

Displaying Object Windows	6-2
Right-Click Menu for All Objects	6-4
Alarms Table	6-4
Nodes Table	6-5
Signaling Points Table	6-8
Linksets Table	6-10
Links Table	6-13
Application Servers Table	6-14
Application Server Processes Table	6-16
Application Server Process Associations Table	6-18
Signaling Gateway Mated Pairs Table	6-19
Interfaces Table	6-21
Cards Table	6-23
RAN Backhauls Table	6-25
RAN Shorthauls Table	6-27
Access Point Names Table	6-29
Software Versions Table	6-30
Point Codes	6-31
IP Addresses	6-31
Editing Properties	6-33
Editing Properties for a RAN-O Backhaul	6-36
Attaching Notes	6-38
Viewing Notes	6-39
Deleting Objects	6-40
Deleting an Object from Your Network	6-40
Deleting an Object from the MWTM Database	6-40
Deleting a Node from the MWTM Discovery Dialog	6-41
Unmanaging and Managing Nodes or ITP Signaling Points	6-42
Excluding Nodes or ITP Signaling Points from a View	6-43
Ignoring and Unignoring Objects	6-43

CHAPTER 7

Managing Views 7-1

Overview	7-1
Default View	7-2

Custom View and Subviews	7-2
Viewing Basic Information for Custom Views	7-2
Right-Click Menu for Views	7-3
Views Summary List Table	7-3
Viewing Detailed Information for Views	7-5
Editing a View	7-6
Saving a View	7-6
Creating a New View	7-8
View Editor Window Menu	7-9
Objects In Current View	7-10
Right-Click Menu for a View	7-11
Right-Click Menu for a Subview	7-11
Right-Click Menu for an Object	7-11
Excluded from View Pane	7-12
New on the Network Pane	7-12
Views List Pane	7-13
View Data Pane	7-13
Directory Listing Pane	7-14
Closing the View Editor Window	7-14
Choosing a View	7-14
Loading the DEFAULT View	7-14
Loading a Client-Specific View	7-15
Ignoring a View	7-16
Viewing Ignored Views	7-16

CHAPTER 8

Understanding Detailed Object Functions 8-1

Viewing the Right-Click Menu for an Object	8-3
Deploying a File Associated with an ITP Node or Signaling Point	8-9
Viewing Management Interfaces and Physical Folders	8-9
Viewing Status Contributors	8-10
Viewing Details	8-12
Address Information	8-14
Advanced Details (Web)	8-14
Association Information	8-14
Bandwidth Information	8-15
Capability Point Code	8-15
Description	8-16
Descriptive Information	8-16

General Information	8-16
Interfaces	8-17
ITP Application Servers	8-17
ITP Linksets	8-18
Interface Information	8-18
IP Addresses for SNMP	8-19
IP Addresses Not for SNMP	8-19
Links Information	8-20
Local IP Address Information	8-20
Naming Information	8-21
Nodes	8-21
Cards	8-22
Interfaces	8-22
ITP Application Servers	8-23
ITP Application Server Processes	8-23
ITP Application Server Process Associations	8-23
ITP Links	8-23
ITP Linksets	8-24
ITP Signaling Gateway-Mated Pairs	8-24
ITP Signaling Points	8-24
Point Code	8-25
Polling Information	8-26
Protection Information	8-27
QoS Information	8-27
RAN Information	8-27
Remote IP Address Information	8-28
Uptime Information	8-28
Status Information	8-28
Nodes	8-29
Interfaces and Cards	8-30
ITP Application Servers	8-34
ITP Application Server Processes	8-35
ITP Application Server Process Associations	8-36
ITP Links	8-38
ITP Linksets	8-39
ITP Signaling Gateway Mated Pairs	8-40
ITP Signaling Points	8-42
Threshold Information (RAN-O Only)	8-43
Viewing Troubleshooting	8-43
Troubleshooting Menu and Toolbar	8-44

Commands That Require Additional User Input	8-45
Viewing Alarms and Recent Events	8-45
Using Provisioning	8-46
Prerequisites for Using Provisioning	8-49
Setting Up the MWTM to Retrieve Running Configuration from the Object	8-49
Using the Provisioning Wizard	8-50
Editing SNMP IP Addresses for a Node	8-51
Polling a Node	8-53
Polling from the Discovery Dialog	8-53
Performing a Normal Poll	8-54
Performing a Clean Poll	8-55
Allowing and Disallowing Trap Processing for a Node	8-56
Viewing Real-Time Data	8-56
Viewing the Syslog	8-57
Viewing CPU Performance	8-58
CPU Processes	8-58
CPU Utilization	8-59
Memory Utilization	8-60
Viewing Trap Settings	8-62
Viewing Data for Interfaces	8-63
Real-Time Interface Performance	8-64
Real-Time Interface Errors	8-65
Viewing Data for ITP Objects	8-66
Charts: Application Servers and Application Server Process Associations	8-68
Charts: Links and Linksets	8-70
Interface Details	8-73
Poll Settings	8-75
Q.752 Measurements	8-76
Right-Click Menu	8-78
SCTP Association Configuration Details	8-78
SCTP Association Statistics Details	8-81
Statistics: Application Servers	8-82
Statistics: Application Server Process Associations	8-82
Statistics: Links and Linksets	8-85
Status Details	8-88
Viewing ITP MTP3 Errors	8-93
Viewing ITP MSU Rates	8-94
Right-click Menu	8-95
Viewing ITP Non-Stop Operation	8-95

Viewing TDM Statistics	8-103
Line Configuration Pane	8-103
Line Status Information Pane	8-106
Performance and Error Information Pane	8-106
Viewing RAN-O Performance Data	8-107
Viewing Shorthaul Performance Data	8-108
Viewing Backhaul Performance Data	8-111
Viewing RAN-O Error Data	8-115
Viewing Shorthaul Errors	8-115
Viewing Backhaul Errors	8-120
Viewing PWE3 Statistics	8-121
Viewing ITP Linkset Access Lists	8-123
Viewing Data Specific for ITP Signaling Points	8-123
Viewing Route Detail	8-124
Viewing GTT MAP Status	8-125
Viewing GTT Statistics	8-126
Viewing the MTP3 Event Log	8-129
Viewing MLR Details	8-130
Viewing MLR Counters	8-130
Viewing MLR Trigger Config	8-132
Viewing MLR Trigger Results	8-136
Viewing RAN Shorthauls	8-140
Creating Virtual RAN Backhauls	8-140

CHAPTER 9

Managing Alarms and Events 9-1

Basic Concepts and Terms	9-1
Event Definition	9-2
Alarm Definition	9-2
Event Processing	9-3
Event Queue Congestion	9-3
Trap Rate Limits	9-3
Database Archiving	9-4
Event Archival Process	9-5
Alarm Archival Process	9-6
File-based Archiving	9-8
Displaying Active Alarms and Event History	9-8
Toolbar Buttons	9-14
Right-click Menus	9-16
Right-Click Menu for All Alarms and Events	9-16

Right-Click Menu for a Specific Alarm or Event	9-17
Managing Filters for Alarms and Events	9-17
Setting an Alarm or Event Filter	9-18
Alarm and Event Filter Buttons	9-19
Properties Settings	9-19
Selected Objects Settings	9-21
Event Filter Example	9-25
Loading an Existing Filter	9-25
Saving a Filter File	9-26
Viewing Properties for Alarms and Events	9-27
Attaching a Note to an Alarm or Event	9-29
Viewing Archived Event Files on the Web	9-30
Viewing the Event Metrics Report on the Web	9-30
Message Types Table	9-31
Message Severity Table	9-31
Status Messages Table	9-32
Trap Messages Table	9-33
Messages/Day Table	9-33
Status Change Messages/Day Table	9-34
SNMP Trap Messages/Day Table	9-34
Files Processed Table	9-34
Date Range Table	9-34
Changing the Way the MWTM Processes Events	9-35
Changing Event Limits	9-37
Specifying a List of SNMP Servers for Trap Forwarding	9-40
Changing Event Categories	9-41
Configuring Trap, Status Alarm, or User Action Events	9-42
Forwarding Events as Traps to Other Hosts	9-48
Setting Sounds for Events at an MWTM Client	9-49
Listing Event Sound Filters	9-49
Creating a New Event Sound Filter	9-50
Adding a Sound File to the MWTM	9-52
Changing an Existing Event Sound Filter	9-53
Deleting an Event Sound Filter	9-53
Playing and Muting Event Sounds	9-53

CHAPTER 10**Viewing Network Topology 10-1**

Topology Menu	10-3

Topology Toolbar Buttons	10-4
Topology Tabs	10-6
Tables Tab	10-6
New Objects Tab	10-9
Excluded Objects Tab	10-10
Topology Map	10-10
Topology Right-Click Menu: Map	10-15
Topology Right-Click Menu: Object	10-15
Topology Alarm Pane	10-16
Creating a Custom Layout	10-16
Finding an Object	10-16
Using the Selection Dialog	10-17
Centering the Topology Map on an Object	10-17
Displaying Detailed Information About a Topology Map Element	10-18
Printing the Topology Map	10-18
Saving the Topology Map as a JPEG File	10-18
Selecting a Directory for the JPEG File	10-19
Activating a Magnetic Grid on the Topology Map	10-20
Specifying a Color for the Magnetic Grid	10-21
Swatches Pane (Recommended)	10-21
HSB Pane	10-21
RGB Pane	10-22
Select Grid Color Field and Buttons	10-22
Specifying a Background Color for the Topology Map	10-22
Swatches Pane (Recommended)	10-23
HSB Pane	10-23
RGB Pane	10-23
Select Background Color Field and Buttons	10-23
Aligning Objects on the Topology Map	10-24
Hiding and Displaying Non-ITP Nodes and Linksets	10-25
Locking and Unlocking the Position of an Icon	10-25
Improving Topology Performance	10-25
Turning Off Antialiasing	10-25
Connecting Locally for Large Networks—Solaris Clients Only	10-26
Hiding and Redrawing Connections When Redrawing	10-26
Hiding and Showing Connections When Redrawing	10-26
Saving the Topology Map	10-26

Restoring the Topology Map 10-27

CHAPTER 11

Accessing Data from the Web Interface 11-1

Accessing the MWTM Web Interface 11-1

Overview of the MWTM Web Interface 11-2

MWTM Web Interface Navigation Tree 11-3

MWTM Web Interface Content Area 11-4

Customizing the Date Range 11-5

Using the Toolbar 11-5

Displaying the Home Page 11-8

Downloading the MWTM Client from the Web 11-9

Downloading the Solaris Client 11-9

Downloading the Windows Client 11-10

Downloading the Linux Client (Unsupported) 11-10

Checking Your Browser 11-10

Accessing Software Updates and Additional Information 11-11

Viewing the MWTM Technical Documentation 11-12

Displaying the Administrative Page 11-12

Viewing System Information for the MWTM 11-14

Viewing System Messages 11-16

Viewing Info Messages 11-16

Viewing Error Messages 11-16

Viewing MWTM User Action Messages 11-17

Viewing All Archived MWTM Messages 11-19

Viewing System Status Information 11-20

Viewing System Status 11-21

Viewing System Versions 11-21

Viewing Connected Clients 11-21

Viewing User Accounts 11-21

Viewing System Logs 11-22

Viewing the Console Log 11-22

Viewing the Command Log 11-23

Viewing the Event Automation Log 11-23

Viewing the Security Log 11-23

Viewing the Install Log 11-24

Viewing the Web Access Logs 11-24

Viewing the Web Error Logs 11-24

Viewing the Report Log 11-25

Viewing Properties 11-25

Viewing System Properties	11-25
Viewing Server Properties	11-27
Viewing Web Configuration Properties	11-27
Viewing Reports Properties	11-29
Viewing Trap Forwarding Properties	11-30
Displaying Alarms and Events	11-30
Displaying Summary Lists	11-31
Displaying Software Versions	11-31
Tools	11-31
Launch Tools	11-32
Search Tools	11-32
Displaying Reports	11-33
Displaying Objects in a View	11-33
Displaying RAN-O Historical Statistics	11-33
Displaying Performance Statistics	11-34
Displaying Shorthaul Performance Statistics	11-35
Displaying Backhaul Performance Statistics	11-36
Displaying Error Statistics	11-39
Displaying Shorthaul Error Statistics	11-40
Displaying Backhaul Error Statistics	11-42
Generating RAN Data Export Files	11-43
Displaying CSG2 Real-Time Statistics	11-44
Global Statistics	11-44
Load Statistics	11-45
BMA Statistics	11-47
Quota Server Statistics	11-48
User Database Statistics	11-49
Displaying BWG Real-Time Statistics	11-49
Global Statistics	11-49
Status	11-50
Creation and Deletion Statistics	11-51
Miscellaneous Statistics	11-52
Signaling Packet Statistics	11-53
DHCP Packet Statistics	11-53
Handoff Statistics	11-54
Data Packet Statistics	11-55
Dropped Packet Statistics	11-56
Profile Statistics	11-57
Rejected Statistics	11-58

Paths Statistics	11-58
User Groups Statistics	11-59
Sessions and Flow Statistics	11-60
Traffic Statistics	11-60
Displaying HA Real-Time Statistics	11-62
Global	11-62
Registrations Processed by AAA	11-62
Registration Requests	11-63
Standby Synchronization	11-63
IP Local Pool Config	11-64
IP Local Pool Stats	11-64
Displaying GGSN Real-Time Statistics	11-65
Global	11-65
GTP Statistics	11-65
Charging Statistics	11-66
GTP Throughput Statistics	11-66
PDP Context Statistics	11-66
AAA Statistics	11-68
IP and UDP Statistics	11-68
SGSN Throughput	11-68
APN General	11-69
APN Miscellaneous Statistics	11-69
APN PDP Context Statistics	11-70
APN Throughput Statistics	11-70
IP Local Pool Config	11-71
IP Local Pool Stats	11-72
Displaying PWE3 Real-Time Statistics	11-72
Displaying TDM Real-Time Statistics	11-72

CHAPTER 12

Managing Reports 12-1

Generating Reports	12-1
Viewing Enabled and Disabled Status for Continuous Reports on the Web	12-2
Generating Custom Statistics Reports	12-3
Including or Excluding Specified Objects in ITP Reports	12-4
Viewing Reports	12-6
Viewing Statistics Reports	12-9
Application Server Reports	12-9
Application Server Process Reports	12-12
Link Reports	12-17

Linkset Reports	12-23
MLR Reports	12-27
MSU Rates Reports	12-32
RAN Reports	12-34
Viewing Accounting Reports	12-41
GTT Accounting Reports	12-41
MTP3 Accounting Reports	12-42
AS/ASP Accounting Reports	12-44
Viewing File Archive Reports	12-45
Custom Archived Reports	12-46
Daily Archived Reports	12-48
Hourly Archived Reports	12-49
Rolling Archived Reports	12-49
Application Server Archived Reports	12-50
Application Server Process Archived Reports	12-50
GTT Accounting Archived Reports	12-51
Link Archived Reports	12-52
Linkset Archived Reports	12-52
MLR Archived Reports	12-53
MSU Archived Reports	12-54
MTP3/AS Archived Reports	12-55
Point Codes Archived Reports	12-58
Q.752 Hourly Archived Reports	12-58
Viewing the MWTM Statistics Reports Logs	12-59
Locating Stored ITP Reports	12-63
Changing the MWTM Reports Directory	12-65
Customizing ITP Report Preferences	12-65

CHAPTER 13

Editing an ITP Route Table File 13-1

Editing an MWTM ITP Route Table File	13-1
Opening a Route Table File from a File	13-2
Opening a Route Table File from a Node	13-3
Opening a Route Table File from an Archive	13-4
Editing ITP Route Tables	13-5
Route Table Dialog Menu	13-7
Route Table Dialog Right-Click Menu	13-8
Route Table	13-8
Loading an Existing Route Table File	13-12
Deploying a Route Table File	13-13

Saving a Route Table File	13-13
Reverting to the Last Saved Route Table File	13-15
Editing a Non-MWTM ITP Route Table	13-16

CHAPTER 14

Editing an ITP Global Title Translation Table 14-1

Launching the GTT Editor	14-2
GTT Menu	14-4
GTT Editor: Selectors and GTA Tab	14-6
Selector Table	14-7
GTA Table	14-8
App Group Table	14-8
MAP Table	14-9
CPC List	14-10
GTT Editor: App Group Tab	14-10
GTT Editor: MAPs Tab	14-11
GTT Editor: CPC Tab	14-12
Concerned Pt. Code Name List	14-13
GTT Editor: Address Conversion Tab	14-13
Address Conversion Table	14-14
Conversion Entry Table	14-14
Selector Table for Address Conversion	14-15
Editing a GTT Table	14-16
Adding a Selector to a Selector Table	14-17
Adding a GTA Entry to a GTT	14-18
Searching the GTA Table for GTA Digits	14-21
Adding an Application Group Entry to an App Group Table	14-23
Adding a MAP Entry to a GTT	14-24
Adding a CPC List to a GTT	14-26
Adding a GTT Address Conversion Table	14-26
Adding an Entry to a GTT Conversion Table Entry	14-28
Deleting Rows from a Table	14-29
Creating a New GTT File	14-30
Loading an Existing GTT File	14-31
Loading a GTT File from a Node	14-33
Loading a GTT File from the Archive	14-34
Displaying the Progress Dialog Box	14-35
Checking the Semantics of a GTT File	14-36

Deploying a GTT File	14-37
Displaying Basic Information About a GTT File	14-38
Supporting Cross-Instance GTT Files	14-39
Network Name Configuration Dialog Box Menu	14-40
Network Name Configuration Dialog Box Table	14-41
Saving a GTT File	14-42
Reverting to the Last Saved GTT File	14-44

CHAPTER 15

Editing ITP MLR Address Table Files	15-1
Launching the Address Table Editor	15-2
Address Table Menu	15-3
Creating a New Address Table File	15-6
Loading an Existing Address Table File	15-8
Loading an Address Table File from a Node	15-10
Loading an Address Table File from the Archive	15-12
Working in Address Table Files	15-14
Result Types and Values	15-15
Editing Address Table Properties	15-17
Checking the Semantics of an Address Table File	15-17
Deploying an Address Table File	15-18
Displaying Basic Information About an Address Table File	15-19
Listing Archived Address Tables	15-20
Creating Network Name Mapping Files	15-20
Network Name Configuration Dialog Menu	15-21
Network Name Configuration Dialog Table	15-22
Saving an Address Table File	15-23
Reverting to the Last Saved Address Table File	15-25

APPENDIX A

Client Object Map Reference	A-1
BWG Node Tabs	A-2
CSG1 and CSG2 Node Tabs	A-3
CSR Node Tabs	A-3
GGSN Node Tabs	A-4
HA Node Tabs	A-4
IP-RAN Node Tabs	A-5
ITP Node Tabs	A-5

mSEF Node Tabs	A-6
ONS Node Tabs	A-6
RAN Service Card Node Tabs	A-7
CDT Node Tabs	A-7
Unknown Node Tabs	A-7
Signaling Point Tabs	A-8
Linkset Tabs	A-9
Link Tabs	A-9
Application Server Tabs	A-9
Application Server Process Tabs	A-10
Application Server Process Association Tabs	A-10
Signaling Gateway-Mated Pair Tabs	A-11
Interface Tabs	A-11
UMTS and GSM Interface Tabs	A-12
Card Tabs	A-12
RAN Backhaul Tabs	A-13
Physical and Management Interface Folder Tabs	A-13

APPENDIX B

Command Reference B-1

General Commands	B-1
mwtm	B-5
mwtm addcreds	B-6
mwtm addsnmpcomm	B-6
mwtm adduser	B-7
mwtm archivedirsize	B-8
mwtm authtype	B-8
mwtm backup	B-9
mwtm backupdays	B-9
mwtm backupdir	B-10
mwtm badloginalarm	B-11
mwtm badlogindisable	B-11
mwtm browserpath	B-12
mwtm certgui	B-12
mwtm certtool	B-12
mwtm changes	B-13
mwtm checksystem	B-13
mwtm clean	B-14
mwtm cleanall	B-14

mwtm cleandb	B-15
mwtm cleandiscover	B-16
mwtm cliconntimer	B-16
mwtm client	B-17
mwtm clientfailoverprompt	B-17
mwtm clientlogs	B-18
mwtm clitimeout	B-18
mwtm cmdlog	B-18
mwtm collectstats	B-19
mwtm confirmfailover	B-20
mwtm console	B-20
mwtm consolelogsize	B-20
mwtm countnodes	B-20
mwtm countobjects	B-21
mwtm cwsetup	B-21
mwtm datadir	B-22
mwtm dbtool	B-23
mwtm delete	B-23
mwtm deletecreds	B-24
mwtm deletesnmpcomm	B-24
mwtm deluser	B-25
mwtm disablepass	B-25
mwtm disableuser	B-26
mwtm discover	B-26
mwtm diskmonitor	B-26
mwtm enableuser	B-27
mwtm eventautolog	B-27
mwtm eventconfig	B-28
mwtm eventeditor	B-28
mwtm eventtool	B-29
mwtm evilstop	B-30
mwtm export	B-30
mwtm export cw	B-31
mwtm help	B-32
mwtm importcw	B-32
mwtm inactiveuserdays	B-32
mwtm installlog	B-33
mwtm inventorytool	B-34
mwtm iosreport	B-35
mwtm ipaccess	B-35

mwtm jspport	B-36
mwtm keytool	B-36
mwtm killclients	B-37
mwtm listusers	B-37
mwtm logger	B-38
mwtm logincreds	B-38
mwtm logsize	B-39
mwtm logtimemode	B-40
mwtm manage	B-40
mwtm maxascirows	B-42
mwtm maxevhist	B-42
mwtm maxhtmlrows	B-43
mwtm mldebug	B-43
mwtm modifysnmpcomm	B-44
mwtm motd	B-44
mwtm msglog	B-45
mwtm msglogage	B-45
mwtm msglogdir	B-46
mwtm netlog	B-46
mwtm netlogger	B-47
mwtm newlevel	B-47
mwtm osinfo	B-47
mwtm passwordage	B-47
mwtm patchlog	B-48
mwtm poll	B-49
mwtm pollertimeout	B-49
mwtm print	B-49
mwtm props	B-50
mwtm provisiontool	B-50
mwtm purgedb	B-51
mwtm readme	B-52
mwtm reboot	B-52
mwtm repdailyage	B-52
mwtm rephelp	B-53
mwtm rephourlyage	B-53
mwtm restart	B-53
mwtm restore	B-54
mwtm restoreprops	B-55
mwtm rootvars	B-55
mwtm sechelp	B-55

mwtm seclog	B-55
mwtm secondaryserver	B-56
mwtm servername	B-57
mwtm setpath	B-57
mwtm showcreds	B-59
mwtm showsnmpcomm	B-59
mwtm snmpcomm	B-59
mwtm snmpconf	B-60
mwtm snmpget	B-60
mwtm snmphelp	B-63
mwtm snmpmaxrows	B-63
mwtm snmpnext	B-63
mwtm snmpsetup	B-65
mwtm snmpwalk	B-66
mwtm sounddir	B-69
mwtm ssl	B-70
mwtm sslstatus	B-71
mwtm start	B-71
mwtm start client	B-71
mwtm start jsp	B-72
mwtm start pm	B-72
mwtm start web	B-72
mwtm status	B-72
mwtm stop	B-72
mwtm stopclients	B-73
mwtm stop jsp	B-73
mwtm stop pm	B-73
mwtm stop web	B-73
mwtm superuser	B-73
mwtm syncusers	B-74
mwtm tac	B-74
mwtm termpoxy	B-75
mwtm trapaccess	B-75
mwtm trapratelimit count	B-76
mwtm trapratelimit interval	B-76
mwtm trapsetup	B-76
mwtm trapstatus	B-77
mwtm tshootlog	B-77
mwtm uninstall	B-78
mwtm unknownage	B-78

mwtm updateuser	B-78
mwtm useraccess	B-79
mwtm userpass	B-79
mwtm version	B-80
mwtm viewlog	B-80
mwtm wall	B-80
mwtm webaccesslog	B-81
mwtm weberrorlog	B-81
mwtm weblogupdate	B-82
mwtm webnames	B-83
mwtm webport	B-83
mwtm webutil	B-84
mwtm who	B-84
mwtm xtermpath	B-84
ITP-Only Commands	B-85
mwtm accstats	B-87
mwtm archivedir	B-88
mwtm atblclient	B-89
mwtm atbldir	B-90
mwtm autosyncconfig	B-91
mwtm chartwindow	B-91
mwtm checkgtt	B-91
mwtm checkmlr	B-92
mwtm checkroute	B-92
mwtm countas	B-92
mwtm countasp	B-92
mwtm countaspa	B-93
mwtm countlinks	B-93
mwtm countlinksets	B-93
mwtm countsgrp	B-93
mwtm countsps	B-93
mwtm deletearchive	B-94
mwtm deployarchive	B-94
mwtm deploycomments	B-95
mwtm evreps clean	B-95
mwtm evreps cleancustom	B-95
mwtm evreps diskcheck	B-95
mwtm evreps enable	B-96
mwtm evreps hourlyage	B-96
mwtm evreps mtp	B-97

mwtm evreps status	B-97
mwtm evreps timer	B-97
mwtm gttclient	B-98
mwtm gttidir	B-98
mwtm gttstats	B-100
mwtm linkstats	B-101
mwtm listarchive	B-103
mwtm listgtt	B-103
mwtm listhistory	B-104
mwtm listmlr	B-104
mwtm listroute	B-104
mwtm mlrstats	B-105
mwtm mtpevents	B-106
mwtm pcformat	B-107
mwtm pclist	B-108
mwtm pushgtt	B-108
mwtm pushmlr	B-109
mwtm pushroute	B-110
mwtm q752stats	B-110
mwtm repcustage	B-112
mwtm repdir	B-112
mwtm replog	B-113
mwtm routedir	B-114
mwtm routetabledefs	B-115
mwtm start atblclient	B-115
mwtm start gttclient	B-116
mwtm statreps acct	B-117
mwtm statreps clean	B-117
mwtm statreps cleancustom	B-118
mwtm statreps custage	B-118
mwtm statreps dailyage	B-119
mwtm statreps diskcheck	B-119
mwtm statreps enable	B-120
mwtm statreps export	B-120
mwtm statreps gtt	B-121
mwtm statreps hourlyage	B-121
mwtm statreps iplinks	B-122
mwtm statreps link	B-122
mwtm statreps maxcsvrows	B-123
mwtm statreps mlr	B-123

mwtm statreps msu	B-124
mwtm statreps nullcaps	B-125
mwtm statreps q752	B-125
mwtm statreps servratio	B-126
mwtm statreps status	B-126
mwtm statreps timemode	B-127
mwtm statreps timer	B-127
mwtm statreps utilratio	B-128
mwtm statreps xua	B-128
mwtm xuastats	B-129
RAN-O-Only Commands	B-130
mwtm rep15minage	B-130
mwtm repmonthlyage	B-131
mwtm statreps 15minage	B-131
mwtm statreps monthlyage	B-132

APPENDIX C**FAQs C-1**

General FAQs	C-1
Installation Questions	C-1
Server Questions	C-2
GUI Questions	C-5
Browser Questions	C-6
Topology Questions	C-6
Events and Alarms Questions	C-7
Polling Questions	C-8
MIB Questions	C-9
Miscellaneous Questions	C-9
ITP Specific FAQs	C-13
RAN-O Specific FAQs	C-17

APPENDIX D**Troubleshooting the MWTM and the Network D-1**

Clearing a Locked-Up MWTM Display	D-1
Investigating Data Problems	D-1
Understanding MWTM Client Start Error Messages	D-2
Data Model Mediator Service Error	D-2
Demand Poller Manager Service Error	D-2
Checking MWTM Server Start Processes	D-3
Viewing the MWTM Troubleshooting Log	D-3

Viewing MWTM Data on the Web	D-4
Troubleshooting IOS Commands on the Web	D-4
Viewing Detailed Troubleshooting Instructions for Events	D-5
Diagnosing a Typical Network Problem	D-5
Diagnosing a Typical ITP Network Problem	D-6
Diagnosing a Typical RAN-O Network Problem	D-8

APPENDIX E

Status Definitions E-1

General Status Definitions	E-1
Status Definitions for Nodes	E-1
Status Definitions for Views	E-2
Status Definitions for Folders	E-2
Status Definitions for Interfaces	E-2
Admin Status	E-2
Operational Status	E-3
Status	E-3
ITP Status Definitions	E-3
Status Definitions for Application Servers	E-4
Status Definitions for Application Server Processes	E-4
Status Definitions for Application Server Process Associations	E-4
Status Definitions for ITP Interfaces	E-5
Admin Status	E-5
Operational Status	E-5
Status	E-6
Status Definitions for Links	E-6
Status Definitions for Linksets	E-7
Status Definitions for Signaling Gateway Mated Pairs	E-7
Status Definitions for Signaling Points	E-7
RAN-O Status Definitions	E-7
Status Definitions for RAN-O Interfaces	E-8
Admin Status	E-8
Operational Status	E-8
Connect State for GSM Abis	E-8
Connect State for UMTS Iub	E-9
Alarm States	E-9
Redundancy State	E-10
Status	E-10
Status Definitions for Cards	E-10
Status Definitions for RAN-O Backhauls	E-10

mSEF Status Definitions	E-10
Status Definitions for APNs	E-10

APPENDIX F**MIB Reference F-1**

BWG Specific MIBs	F-1
Common MIBs	F-2
CSG1 Specific MIBs	F-5
CSG2 Specific MIBs	F-6
GGSN Specific MIBs	F-6
HA Specific MIBs	F-7
ITP Specific MIBs	F-8
IPRAN Specific MIBs	F-10

APPENDIX G**Trap Reference G-1**

General Traps	G-1
ITP Specific Traps	G-7
IPRAN Specific Traps	G-11
RAN-O Specific Traps	G-11
PWE3 Specific Traps	G-12
mSEF Specific Traps	G-12
Generic mSEF Traps	G-13
CSG1 Traps	G-14
CSG2 Traps	G-15
GGSN Traps	G-16
BWG Traps	G-18
HA Traps	G-19

APPENDIX H**Configuring MWTM to Run with Various Networking Options H-1**

How Does RMI Work?	H-2
VPN Communication	H-3
NAT Communication	H-5
Firewall Communication	H-6
Configuring Port Numbers and Parameters	H-7
Configuring Firewalls	H-8
Sample Firewall Configuration	H-10
Port-Forwarding Communication	H-12
Configuring MWTM to Work With a Dual-Interface Machine Connected to Separate Networks	H-14

MWTM Server Configuration	H-15
MWTM Client A Configuration	H-16
MWTM Client B Configuration	H-16
Additional Network Configurations	H-17
SSL Communication	H-17
Configuring MWTM with IOS Server Load Balancing	H-18

APPENDIX I

MWTM Ports	I-1

INDEX



About This Guide

This preface describes the objectives, audience, organization, and conventions of the *User Guide for the Cisco Mobile Wireless Transport Manager 6.1*. It refers you to related publications and describes online sources of technical information.

The Cisco Mobile Wireless Transport Manager (MWTM) is a network management software product that enables you to discover, manage, and troubleshoot the following networks:

- IP Transfer Point (ITP)
- IP Radio Access Network (IPRAN), which includes:
 - Radio Access Network Optimization (RAN-O)
 - Pseudowire Emulation Edge to Edge (PWE3)
- Cisco Mobile Internet (MI) / mobile Services Exchange Framework (mSEF), which includes:
 - Cisco Gateway GPRS Support Node (GGSN)
 - Cisco Content Services Gateway (CSG)
 - Cisco Home Agent (HA)
 - Cisco Broadband Wireless Gateway (BWG)

For a more detailed description of the MWTM, see [Chapter 1, “Overview.”](#) For the latest MWTM information and software updates, go to <http://www.cisco.com/go/mwtm>.

This preface includes:

- [Document Objectives, page xxxi](#)
- [Document Audience, page xxxii](#)
- [Document Organization, page xxxii](#)
- [Document Conventions, page xxxiii](#)
- [Related Documentation, page xxxiv](#)
- [Obtaining Documentation and Submitting a Service Request, page xxxv](#)

Document Objectives

This guide describes the architecture, supporting hardware and software, and management procedures for the MWTM. Using the information provided in this guide, you can complete the tasks that are necessary to use the MWTM in your ITP, RAN-O, and/or mSEF network.

Document Audience

This guide is for network administrators or operators who use the MWTM software to manage ITP, RAN-O, and/or mSEF networks. Network administrators or operators should have:

- Basic network management skills
- Basic Solaris system administrator skills
- Basic ITP, RAN-O, and/or mSEF knowledge

Document Organization

This guide is divided into the following chapters and appendixes:

- [“Overview”](#) provides brief descriptions of ITP, RAN-O, and mSEF, the MWTM, the MWTM’s client-server architecture, and an overview of how to use the MWTM to manage your network.
- [“Configuring Security”](#) provides information about configuring MWTM security and limiting access to the MWTM.
- [“Setting Up Your Server”](#) provides procedures to setup your MWTM server, which includes enabling traps, configuring a backup server, setting up TFTP, configuring SNMP settings and credentials, and creating new troubleshooting commands.
- [“Getting Started”](#) provides basic information and procedures for using the MWTM.
- [“Basic Operations”](#) provides information about basic operations you can perform using the MWTM, including navigating windows, exporting data, and performing basic server operations.
- [“Understanding Basic Object Functions”](#) provides information about basic object functions found within the Summary Lists section of the navigation tree.
- [“Managing Views”](#) provides information about using the MWTM to create, change, and load views and subviews, and view basic and detailed information for views and subviews.
- [“Understanding Detailed Object Functions”](#) provides information about more detailed object functions you can perform on specific types of objects.
- [“Managing Alarms and Events”](#) provides information about using the MWTM to view basic and detailed information for events, and change the way the MWTM processes events.
- [“Viewing Network Topology”](#) provides procedures for viewing the topology of your network, changing the way the MWTM shows the topology, and saving customized topology displays.
- [“Accessing Data from the Web Interface”](#) describes how to access MWTM data from the MWTM Web interface.
- [“Managing Reports”](#) provides procedures for creating and viewing MWTM accounting and statistics reports for your ITP network.
- [“Editing an ITP Route Table File”](#) provides procedures for viewing and editing ITP route table files.
- [“Editing an ITP Global Title Translation Table”](#) provides procedures for viewing and editing ITP GTT files.
- [“Editing ITP MLR Address Table Files”](#) provides procedures for viewing and editing ITP MLR address table files.
- [“Client Object Map Reference”](#) provides an overview of the tabs available for each MWTM object within a view.

- “[Command Reference](#)” describes the commands used to set up and operate the MWTM.
- “[FAQs](#)” provides a list of frequently asked questions and troubleshooting tips for the MWTM.
- “[Troubleshooting the MWTM and the Network](#)” provides information for troubleshooting basic MWTM and network problems, including how to verify network discovery, clearing a locked-up MWTM display, and using the MWTM to diagnose typical network problems.
- “[Status Definitions](#)” defines the default status settings for all MWTM network objects.
- “[MIB Reference](#)” lists and describes the MIB variables that are polled by the MWTM.
- “[Trap Reference](#)” lists and describes the traps that the MWTM supports.
- “[Configuring MWTM to Run with Various Networking Options](#)” describes communication between the MWTM client and the MWTM server in different networking environments, including Virtual Private Network (VPN), Network Address Translation (NAT), firewall, port-forwarding, and Secure Sockets Layer (SSL).
- “[MWTM Ports](#)” lists MWTM services ports, port type and descriptions.

Document Conventions

This guide uses basic conventions to represent text and table information.

Command descriptions use the following conventions:

- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([]) are optional.
- Alternate but required keywords are grouped in braces ({ }) and separated by a vertical bar (|).

Examples use the following conventions:

- Terminal sessions and information that the system displays are printed in `screen` font.
- Information that you enter is in **boldface screen** font. Variables for which you enter actual data are printed in *italic screen* font.
- Nonprinting characters, such as passwords, are shown in angle brackets (< >).
- Information that the system displays is in `screen` font, with default responses in square brackets ([]).

This publication also uses the following conventions:

- Menu items and button names are in **boldface** font.
- Directories and filenames are in *italic* font.
- If items such as buttons or menu options are dimmed on application windows, it means that the items are not available either because you do not have the correct permissions or because the item is not applicable at this time.



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in the manual.



Caution

Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

**Tip**

Means the following are useful tips.

Related Documentation

Related MWTM documentation includes:

- [Additional MWTM Documentation, page xxxiv](#)
- [ITP Documentation, page xxxiv](#)
- [IPRAN Documentation, page xxxiv](#)
- [mSEF Documentation, page xxxv](#)

Additional MWTM Documentation

Additional MWTM documentation can be found on Cisco.com:

http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html

The MWTM includes a browser-based online help system that is searchable and supports bookmarking of favorite content.

**Note**

When you access online help for the first time, there might be a slight pause while your client browser loads the online help.

ITP Documentation

Information about Cisco IP Transfer Point (ITP) software, including procedures for configuring ITP objects, can be found on Cisco.com:

http://www.cisco.com/en/US/products/sw/wirelssw/ps1862/products_feature_guides_list.html

Information about the Cisco ITPs can be found in the documentation that shipped with the ITP.

IPRAN Documentation

Information about Cisco IPRAN nodes, including procedures for configuring IPRAN objects, can be found on Cisco.com:

- http://www.cisco.com/en/US/products/hw/routers/ps4062/products_installation_and_configuration_guides_list.html
- http://www.cisco.com/en/US/products/hw/optical/ps2006/products_installation_and_configuration_guides_list.html

CiscoWorks LMS Documentation

Information about the CiscoWorks LAN Management Solution (LMS) 3.1 products, which can be integrated with the MWTM, can be found on Cisco.com:

- http://www.cisco.com/en/US/products/sw/cscowork/ps2425/tsd_products_support_series_home.html

mSEF Documentation

Information about mSEF documentation can be found on Cisco.com:

- GGSN—http://www.cisco.com/en/US/products/sw/wirelssw/ps873/tsd_products_support_series_home.html
- CSG—http://www.cisco.com/en/US/products/sw/wirelssw/ps779/tsd_products_support_series_home.html
- HA—http://www.cisco.com/en/US/products/ps5940/tsd_products_support_series_home.html
- BWG—<http://www.cisco.com/en/US/products/ps8738/index.html>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

Overview

This chapter describes the Cisco Mobile Wireless Transport Manager (MWTM) and contains:

- [What Is the MWTM?, page 1-1](#)
- [What Is ITP?, page 1-6](#)
- [What is CDT?, page 1-7](#)
- [What is IPRAN?, page 1-7](#)
- [What is PWE3?, page 1-8](#)
- [What Is RAN-O?, page 1-8](#)
- [What Is mSEF?, page 1-9](#)
- [How Do I Identify My Network Type?, page 1-9](#)
- [What Is Client/Server Architecture?, page 1-10](#)

What Is the MWTM?

Using the MWTM, you can discover, manage, and troubleshoot objects in your ITP, IPRAN, and/or mSEF network. The MWTM provides:

- [Server and Network Features, page 1-2](#)
- [Graphical User Interface and Web Features, page 1-2](#)
- [Event Monitoring Features, page 1-3](#)
- [Performance Features, page 1-3](#)
- [Provisioning Features, page 1-3](#)
- [Security Features, page 1-4](#)
- [Topology Features, page 1-4](#)
- [Troubleshooting Features, page 1-4](#)
- [Customization Features, page 1-5](#)
- [Integration Features, page 1-5](#)

Server and Network Features

The MWTM:

- Uses client/server architecture. See [What Is Client/Server Architecture?](#), page 1-10 for more details.
- Supports Windows and Solaris clients and Solaris and Linux servers, and provides data access through a Web browser.
- Supports large networks and is verified to work with a network containing more than 1,000 cell sites, or 150 Cisco ITP nodes and 20 clients connected to the server.
- Allows multiple MWTM servers to monitor the network simultaneously, providing data redundancy. Clients have server failure recognition and automatic failover capabilities. MWTM clients will automatically switch to a backup server when the primary server is not available (in network problems or hardware failures, for example).
- Discovers the entire Cisco ITP network and displays the ITP nodes, neighboring SS7 equipment, and linksets in tables and in a network topology drawing that you can customize.
- Discovers the entire Cisco IPRAN network. Displays the RAN-O network element, neighboring equipment, and physical and logical connections in a network topology drawing that you can customize.
- Discovers the mobile Services Exchange Framework (mSEF), including:
 - Cisco Gateway GPRS Support Node (GGSN)
 - Cisco Content Services Gateway (CSG)
 - Cisco Home Agent (HA)
 - Cisco Broadband Wireless Gateway (BWG)
- Lets you create custom views and subviews for grouping similar nodes together, where the state of the subview is the aggregation of the states of the contained nodes.
- Provides a command-line interface (CLI) on the server.
- Allows clients to connect to a server through the IP network; clients work across a Virtual Private Network (VPN) connection through a firewall that supports port forwarding or Network Address Translation (NAT), and through a Secure Sockets Layer (SSL) connection.
- (ITP only) Supports concurrent network indicators and variants; ANSI, China, ITU, NTT, and TTC point code variants; three- and four-octet point code formats; multiple secondary point codes; SS7 instance translation; and virtual linksets.

Graphical User Interface and Web Features

The MWTM:

- Provides a Java-based, easy-to-use GUI on the client with an easy-to-navigate *tree* display of all network objects as well as extensive web-based online help.
- Provides an extensive HTML-based web interface. Most of the primary GUI client features are also available on the web interface except the topology map, real-time data charts, and event management (and, for ITP networks, route table and GTT file configuration).

Event Monitoring Features

The MWTM:

- Displays a real-time event list that supports acknowledgement, annotation, customized filtering, and field viewing that conform to ITU-T Q.733 standards.
- Receives native traps from nodes in the Cisco IPRAN, Cisco mSEF and Cisco ITP solutions and uses SNMP polling to identify the status of each managed node, including interfaces, links, and circuits. The MWTM uses easy-to-recognize, color-coded icons to report the status.
- Monitors Cisco ITP nodes running Message Transfer Part Level 3 (MTP3) User Adaptation (M3UA) or Signaling Connection Control Part (SCCP) User Adaptation (SUA) application servers, as well as servers with multiple signaling points or variants acting as gateways.
- Provides web-based status monitoring, alarm viewing, sorting, filtering, archiving, online documentation, and client download.
- Provides external script execution on the server and sound playing on the client; both are triggered by events or alarms, and you can also customize them.

Performance Features

The MWTM:

- Provides extensive web-based accounting and network statistics reports for:
 - **Cisco RAN-O nodes**—Network utilization and detailed interface-level statistics
 - **Cisco ITP nodes**—Network efficiency, detailed interface-level statistics, Q.752-based statistics reports, and point code inventory reports, including MTP3, GTT, M3UA/SUA, MSU, and multilayer routing reports
- Displays real-time data rate and usage line graphs
- Supports options to configure collection intervals, record aging and statistics export via comma-separated values (CSV) format files

Provisioning Features

The MWTM provides provisioning for ITP, IPRAN, GGSN and CSG.

The MWTM:

- ITP—Assists in provisioning destination point code (DPC) route tables, global title translation (GTT) tables, multilayer routing (MLR) address tables, links and linksets by providing GUI-based editing; reduces errors by checking syntax and semantics before deploying the tables to the Cisco ITP node.
- ITP—Provides revision management and archiving of DPC route, GTT, and MLR address tables; can re-deploy a known good configuration in the event of a misconfiguration. Stores time of change, user ID, and comments for each change.
- ITP—Provides a deployment wizard that simplifies the process of transferring and activating GTT and DPC route-table configuration files onto Cisco ITP nodes. The wizard takes you through deployment step-by-step and learns along the way to speed up future deployments.
- IPRAN—Provides a deployment wizard for PWE3 circuits, ATM cell switching, and TDM drop and insert provisioning.

- GGSN—Provides a deployment wizard for APNs, interfaces, VLANs, and VRFs. These features are available for GGSN 8 and later software.
- CSG—Provides a deployment wizard for Maps, Content, Service, Billing, and Policies. These features are available for CSG2 R1 and later software.

Security Features

The MWTM provides:

- Management of SSL certificates via the GUI
- Multi-level password-protected access for multiple users
- Multiple user authentication methods (OS-based and standalone)
- Passwords that users can change using the GUI
- Password enforcement policies (aging, minimum length, and lockouts)
- Audit trails of all user actions and all access via the web interface
- Security logs
- Optional access via VPN, Secure Shell (SSH), and SSL

Topology Features

The topology features are available for the ITP and RAN-O solutions.

The MWTM:

- Automatically discovers the network from any node, with links to unsupported nodes, and creates topological (graphical) and tabular (text) views of the network.
- Shows network objects as color-coded glyphs on a topology map, with right-click menus and layout, zoom, find, grid, hide, show, and save-as-JPEG functions. The topology map can be organized into one or more submaps, with a single object representing groups of network objects on the main topology map.
- Shows detailed data (including alarm and node data) in columns that can be resized, sorted, or hidden, depending on your preferences.

Troubleshooting Features

The MWTM provides:

- Troubleshooting tools that you can customize to help reduce the total time to resolution of network or node problems
- Integrated, online, context-sensitive help

Customization Features

The MWTM:

- Automatically saves your preferences, such as the size of specific windows or the order of columns in a window, and automatically applies those preferences whenever you launch the MWTM client.
- Polls the nodes on demand and at user-defined intervals, and reports the real-time status of all network objects and events, including the reason for any changes in status.
- Receives SNMP traps natively to drive alarms, and accurate and up-to-date status displays.

You can:

- Customize MWTM network(s) to show menus, options, and tools that are specific to the types of network that you are managing. You customize your network preferences during installation. You can change the network type later, if required, through the command line.
- Customize the GUI, topology, and tabular views to meet your specific needs. You can save customized views and subviews for future use and reference, and share them with other network users.
- Annotate network objects and events, attaching important information such as detailed descriptions, locations, service history, what triggered the event, and how often it has occurred.
- Customize the display category, severity, color, and message that you see with events. You can even have the MWTM play unique sounds for different types of events.
- Automate events, calling UNIX scripts to drive automatic paging, e-mail, and so on.
- Forward SNMP traps, and MWTM events in the form of SNMP traps, to other hosts, such as the Cisco Info Center (CIC) and the Micromuse Netcool suite of products.
- (ITP only) Load destination point code (DPC) route tables, GTT tables, and MLR address tables from files or from ITPs, configure the tables in the MWTM client, and deploy and activate the tables on ITPs. Supports GTT file format versions 3.1, 4.0, and 4.1. Supports cross-instance GTT files. Provides command-line verification of route tables and GTT tables.

Integration Features

The MWTM can integrate with:

- CiscoWorks LAN Management Solution (LMS) portal, which provides a suite of CiscoWorks products, including:
 - Resource Manager Essentials, which provides network management for Cisco ITP, RAN-O, and mSEF nodes.
 - CiscoView Element Manager, which provides dynamic status, monitoring, and configuration information for a broad range of Cisco internetworking products.
- CiscoView element manager and the CiscoWorks Device Center, which you can launch from the:
 - Main window when you right-click a node in the navigation tree.
 - Topology map for quick drill-down network analysis.
- CSG Service Manager for provisioning and service activation of CSG features in the network.
- GGSN Service Manager for provisioning and service activation of GGSN features in the network.

- The Cisco Transport Controller (CTC) on the Cisco Optical Networking System (ONS) 15454 for managing alarms and provisioning circuits on the SONET or SDH traffic cards. You can launch the CTC from a right-click menu in the MWTM client.

The MWTM:

- Receives SNMP traps and generates Cisco MWTM-specific traps for forwarding to external SNMP-based network management applications such as Cisco Info Center or IBM Tivoli/NetCool.
- Stores statistics in CSV format files for extracting performance and key performance indicators.
- Processes northbound Cisco ITP, mSEF, and IPRAN events, inventory, and provisioning XML/SOAP APIs, allowing 3rd-party OSSs to programmatically manage:

Events	• Retrieving all or filtered list of events (based on time, event ID, severity, category, message text) • Clearing event alarms • Changing event severity • Acknowledging events • Attaching text notes to events
Inventory	• Retrieving all inventory objects • Retrieving a specific inventory object • Walking the MWTM inventory tree • Attaching text notes to an inventory object
Provisioning (ITP only)	• Customizing the MWTM templates when necessary • Configuring: – linksets – links – application servers – application server processes

What Is ITP?

The Cisco hardware and software SS7-over-IP (SS7oIP) solution includes the ITP, which provides a reliable, cost-effective medium for migrating Signaling System 7 (SS7), the telecommunications network signaling technology, to the mobile wireless industry IP environment. The ITP off-loads SS7 traffic onto the IP network, replacing the mobile service provider's signaling network with a redundant IP cloud.

In the ITP, and in the MWTM, a *node* is a Cisco ITP or a legacy SS7 device (SSP, SCP, or STP).

A Cisco ITP node can have multiple *signaling points*. Signaling points are identified with unique addresses called *point codes*. Point codes are carried in signaling messages that are exchanged between signaling points to identify the source and destination of each message.

Signaling points and legacy SS7 nodes are connected by *links*, and multiple links are grouped in a *linkset*. Each link is assigned to a single linkset, but each linkset can have multiple links. Links within the same linkset must be parallel between the same signaling points or nodes.

In the MWTM, a linkset is a representation of *two* linksets that are associated with two signaling points or nodes, one for each side of a logical connection.

An *application server* is a logical entity serving a specific routing key.

The application server implements a set of one or more unique *application server processes*, of which one or more is normally actively processing traffic. An application server process is an IP-based instance of an application server, such as Call Agents, HLRs, SMSCs, and so on. An application server process can implement more than one application server.

An *application server process association* is the ITP virtual view of an application server process. The application server process association resides and is defined on the ITP.

A *signaling gateway-mated pair* is a pair of signaling gateways that exchange necessary state information by using the Signaling Gateway Mate Protocol (SGMP).

Collectively, nodes, signaling points, linksets, links, application servers, application server processes, application server process associations, and signaling gateway-mated pairs are known as *managed objects*.

For more information about ITP, including procedures for configuring ITP objects, see the *IP Transfer Point (ITP)* feature module for Cisco IOS software release 12.2(25)SW5 or later.

What is CDT?

The Cisco Database for Telecommunications (CDT) is a per subscriber routing solution that supports SS7/C7 and IP-based addressing services. Alarming is provided by the master server (monitored by MWTM). An alarm event consists of a component (service or facility) name, class, and severity level, as well as detailed message information. System events include resource thresholds (throughput, database capacity, thread utilization, etc.), network connectivity, user authentication, system availability, etc.

You can use the MWTM to discover CDT nodes and provide basic monitoring functions such as alarm status, polling information, and recent events. From the MWTM, you can launch the CDT login web page.



Note

MWTM 6.1 supports CDT 2.0. For SNMP traps to be handled properly CDT must be configured to use SNMPv2 traps.

What is IPRAN?

The Cisco IP Radio Access Network (IPRAN) delivers standards-based end-to-end, IP connectivity for RAN transport. The Cisco solution converts RAN voice and data frames into IP packets at the cell site, and transports them seamlessly over a backhaul network. At the central site, the RAN frames are extracted from IP packets, and the ATM or TDM streams are rebuilt. The result is a transparent, radio vendor-agnostic, RAN IP transport solution.

The Cisco IPRAN solution is also known as Mobile Transport over Pseudowires, or MTOP. For more information about MTOP, see:

http://www.cisco.com/en/US/netsol/ns732/networking_solutions_solution.html

There are two families of pseudowire protocols used within the Cisco IPRAN: PWE3 and RAN-O.

What is PWE3?

Pseudowire Emulation Edge to Edge, or PWE3, is the emulation of an ATM or TDM service over IP, MPLS, or L2TPv3 transport. The PWE3 protocol family is used to encapsulate RAN voice and data frames at the cell site for transport over a backhaul network.

Cisco nodes that support PWE3 and are managed by MWTM include:

- Cell Site Router (CSR):
 - Cisco MWR1941-DC-A router
 - Cisco 3825 Integrated Services router
- Cisco 7600 router

What Is RAN-O?

Radio Access Network Optimization (RAN-O) delivers standard-based, end-to-end, IP connectivity for GSM and UMTS RAN transport. The solution Cisco offers frames RAN voice and data frames into IP packets at the cell-site, and transports them seamlessly over an optimized backhaul network. At the central site, the RAN frames are extracted from IP packets and the Abis or Iub data streams are rebuilt. The result is a transparent, radio vendor-agnostic, RAN IP transport and optimization solution that delivers nominal optimization efficiency of 50% without any impact on voice quality.

In RAN-O and in the MWTM, a *node* is a Cisco RAN-O device. A RAN node can be one of the following:

- Cell Site Router (CSR):
 - Cisco MWR 1941-DC-A router
 - Cisco 3825 Integrated Services Router
- Cisco ONS 15454 SONET multiplexer
- RAN Service Module (card in the Cisco ONS 15454 SONET multiplexer)
- Unmanaged RAN node (BSC, RNC, BTS, or Node B)

**Note**

The MWTM does not manage BSC, BTS, RNC, or Node B objects but displays them in the topology window to help you visualize the network.

RAN interfaces that are available on the nodes interconnect nodes in a RAN-O network. A Cisco RAN-O node can have multiple *RAN interfaces*.

Cards are the modules that reside in the Cisco ONS 15454 SONET multiplexer.

IP backhauls are the trunks that transport optimized voice and data traffic between a remote cell-site RAN-O node and an aggregation RAN-O node at a central site.

RAN shorthauls are the interfaces that transport GSM or UMTS voice and data traffic between the Base Transceiver Station (BTS) or Node-B and the RAN-O node at the cell site. At the aggregation site, RAN shorthauls exist between the RAN-O node and the BSC or RNC.

RAN backhauls describe the end-to-end RAN connections between the BTS or Node-B at the cell site and the BSC or RNC at the aggregation site.

Collectively, nodes, interfaces, cards, and RAN backhauls and shorthauls are known as *managed objects*.

For more information about RAN-O objects, see:

- *Cisco MWR 1941-DC-A Mobile Wireless Edge Router Software Configuration Guide:*
http://www.cisco.com/en/US/products/hw/routers/ps4062/products_configuration_guide_chapter09186a00804d45e1.html
- *Cisco ONS 15454 RAN Service Module Software Configuration Guide:*
http://www.cisco.com/en/US/products/hw/optical/ps2006/products_configuration_guide_book09186a0080787fc2.html

What Is mSEF?

The Cisco Mobile Internet, also known as mobile Services Exchange Framework (mSEF), provides standards-based framework to enable the mobile Internet that links the RAN to IP networks and the services they provide. The mSEF provides:

- Access and service activation
- Easy mobility
- Packet inspection

The mSEF gateways that the MWTM manages include:

- Cisco Content Services Gateway (CSG)
 - CSG1 provides CSG features on the CSG card
 - CSG2 provides the latest CSG features on the Service and Application Module for IP (SAMI)
- Cisco Gateway GPRS Support Node (GGSN) on the SAMI and Multiprocessor WAN Application Module (MWAM)
- Cisco Home Agent (HA) on the SAMI and Cisco 7301
- Cisco Broadband Wireless Gateway (BWG) on the SAMI and Cisco 7301

For more information about mSEF, see:

http://www.cisco.com/en/US/netsol/ns706/networking_solutions_solution_category.html

How Do I Identify My Network Type?

The MWTM can manage one or more types of networks. To determine the type of network that the MWTM is managing, launch the MWTM (by using either the MWTM client or web interface), and observe the network type or types in the title bar. For example, if the MWTM is managing all network types, the title bar displays *(RAN-O ITP CSG1 CSG2 GGSN HA BWG)*.

You can also click on a node in the left tree of the MWTM main window to view detailed information about the node in the right pane. The Node Type and other information provide enough details to determine the type of network you are managing.

If you are using the MWTM to manage multiple network types, you can uniquely identify node types by the DNS host names that you assign to them. For example, you can incorporate the string *itp* into the host name of an ITP node (as in *itp-75*). Similarly, IPRAN nodes can employ a unique host naming scheme (for example, *rano-34*). In addition, you can segregate the nodes of different network types into different management subviews with, for example, one subview for ITP and another subview for IPRAN nodes. For more information about creating views and subviews, refer to [Chapter 7, “Managing Views.”](#)

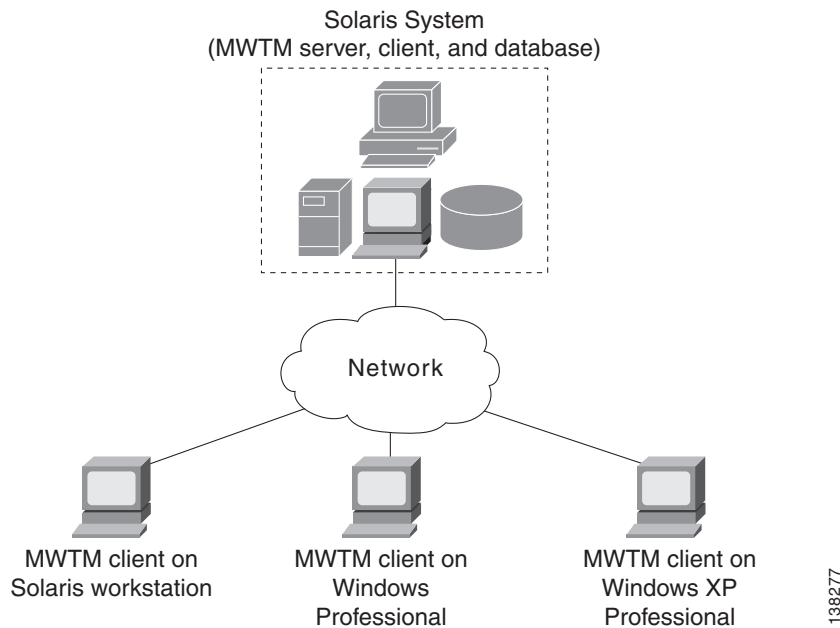
What Is Client/Server Architecture?

The MWTM provides central services and database functions on an MWTM server, which communicates through a messaging interface with multiple MWTM clients.

The MWTM supports a maximum of 20 clients per MWTM server.

The MWTM comprises server and client software components that can be installed on the same workstation or on different workstations. The MWTM server is currently available on Solaris or Linux. The MWTM client is available on Solaris and Windows XP Professional.

Figure 1-1 MWTM Client/Server Architecture



Note

The MWTM client is also available on Linux, but is not a supported feature of the MWTM. Use it under advisement.

The client/server architecture is cross-platform compatible, with which you can run the client and server software in mixed operating system environments. For example, you can run the MWTM server on a Solaris or Linux workstation, and access it from an MWTM client running on Windows XP Professional.

The MWTM server software comprises a group of functional services that manage the data among the network, client workstations, and the centralized database. The MWTM server manages the exchange of data between the MWTM database and the network nodes. The MWTM process manager launches and manages all of the MWTM server processes, providing a robust and reliable launching platform for the MWTM.

The MWTM client software communicates with the MWTM server. You can install the MWTM client software on the same workstation as the MWTM server software, or on a different workstation on the same network as the MWTM server. After you install the MWTM server, you can download the MWTM client software from the web, for easy distribution to users and easier access to important information.

**Note**

For detailed information on installing the MWTM server and client software, refer to the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.



CHAPTER 2

Configuring Security

Before you set up your server for discovering, monitoring, and configuring your Cisco network, you need to make some decisions about the level of security you desire in your network management. With the Cisco Mobile Wireless Transport Manager (MWTM), you can determine how you want users to authenticate, whether you want encrypted data between the application client and the server, and if you want to limit client access to specific IP addresses.

This chapter provides information about configuring MWTM security and limiting access to the MWTM:

- [Configuring User Access, page 2-1](#)
- [Implementing SSL Support in the MWTM, page 2-22](#)
- [Limiting MWTM Client Access to the MWTM Server \(Server Only\), page 2-31](#)
- [Backing Up or Restoring MWTM Files \(Server Only\), page 2-32](#)
- [Removing MWTM Data from the MWTM Server, page 2-35](#)

Configuring User Access

You can use the MWTM to control who is allowed to do what in the MWTM, beyond simply specifying root and nonroot users. The MWTM calls this ability user-based access.

User-based access provides multilevel, password-protected access to MWTM features. Each user can have a unique user name and password. You can also assign each user to one of five levels of access, which control the list of MWTM features accessible by that user.

To configure MWTM user access, perform the tasks in the following sections. Required and optional tasks are indicated:

Required:

- [Implementing Secure User Access \(Server Only\), page 2-2](#)
- [Creating Secure Passwords, page 2-7](#)
- [Configuring MWTM User Account Levels \(Server Only\), page 2-7](#)

Optional:

- [Automatically Disabling Users and Passwords \(Server Only\)](#), page 2-11
- [Manually Disabling Users and Passwords \(Server Only\)](#), page 2-13
- [Enabling and Changing Users and Passwords \(Server Only\)](#), page 2-14
- [Displaying a Message of the Day \(Server Only\)](#), page 2-16
- [Manually Synchronizing Local MWTM Passwords \(Server Only\)](#), page 2-17
- [Listing All Currently Defined Users \(Server Only\)](#), page 2-18
- [Displaying the Contents of the System Security Log \(Server Only\)](#), page 2-18
- [Restoring Security-Related MWTM Data \(Server Only\)](#), page 2-19
- [Disabling MWTM User-Based Access \(Server Only\)](#), page 2-20
- [Specifying a Super User \(Server Only\)](#), page 2-20

Implementing Secure User Access (Server Only)

Before you can access the full suite of security commands in the MWTM, you must enable MWTM user access, configure the type of security authentication you want, and add users to your user lists.

After you implement user access for the MWTM, users must log in to the system to access the:

- MWTM client interface
- MWTM web interface
- Event Editor
- Global Title Translation (GTT) Editor (ITP only)
- Address Table Editor (ITP only)

**Note**

After you implement MWTM user access, if a user logs in on one client, then logs in on a second client, the MWTM closes the first client and records the event in the system security log.

Security Authentication

Two types of security authentication are possible:

- *Local authentication:* You can create user accounts and passwords that are local to the MWTM system. When using this method, you can use MWTM user access commands to manage user names, passwords, and access levels.
- *Solaris/Linux authentication:* Uses standard Solaris- or Linux-based user accounts and passwords, as specified in the `/etc/nsswitch.conf` file. You can provide authentication using the local `/etc/passwd` file; a distributed Network Information Services (NIS) system; or any other type of authentication tool (for details, see [Additional Authentication Tools](#), page 2-3). You can use all MWTM user access commands except:
 - `mwtm disablepass`
 - `mwtm passwordage`
 - `mwtm userpass`

In addition, if you have enabled Solaris/Linux authentication, you must be logged in as the root user, not as a superuser, to use:

- mwtm adduser
- mwtm updateuser
- mwtm authtype



Note When using the solaris or linux options, you must enable SSL (see [Implementing SSL Support in the MWTM, page 2-22](#)).

Additional Authentication Tools

With the introduction of Pluggable Authentication Modules (PAM) in MWTM 6.1, you can use additional authentication tools, such as Remote Authentication Dial In User Service (RADIUS) or Terminal Access Controller Access-Control System (TACACS+).

For example, say you want to use RADIUS. Here's how you would proceed:

-
- Step 1** Ensure that you have:
- Selected Solaris or Linux authentication, either during installation or using the mwtm authtype command (see [mwtm authtype, page B-8](#))
 - Downloaded and compiled the PAM radius module from the internet

- Step 2** On the MWTM server, copy the PAM radius file (*pam_radius_auth.so*) you downloaded to the /usr/lib/security directory.

- Step 3** For Solaris authentication:

- a. On the MWTM server, using a text editor, open this file:

```
/etc/pam.conf
```

- b. Modify these lines:

```
mwtm-jpam auth required pam_unix_auth.so
mwtm-jpam account required pam_unix_account.so
```

to:

```
mwtm-jpam auth required pam_radius_auth.so
mwtm-jpam account required pam_radius_auth.so
```

For Linux authentication:

- a. On the MWTM server, using a text editor, open this file:

```
/etc/pam.d/mwtm-jpam
```

- b. Modify these lines (for 32 or 64-bit, respectively):

```
auth required /lib/security/pam_unix_auth.so
account required /lib/security/pam_unix_auth.so
or
auth required /lib64/security/pam_unix_auth.so
account required /lib64/security/pam_unix_auth.so
```

to:

```
auth required /lib/security/pam_radius_auth.so
account required /lib/security/pam_radius_auth.so
```

```
or
auth required /lib64/security/pam_radius_auth.so
account required /lib64/security/pam_radius_auth.so
```

- Step 4** Enter:
- ```
cd /etc
```
- Step 5** Create the following directory: *raddb*.
- Step 6** You should have a PAM configuration file named *pam\_radius\_auth.conf*. Copy this file as *server* in the */etc/raddb/* directory.
- Step 7** Configure the *server* file you just created with the actual Radius server, port number, and the secret password. For example:
- ```
172.16.24.60:1812 secret 3
```
-

User Levels

You can configure one of five account levels for each user. Valid levels are:

1. [Basic User \(Level 1\) Access](#)
2. [Power User \(Level 2\) Access](#)
3. [Network Operator \(Level 3\) Access](#)
4. [Network Administrator \(Level 4\) Access](#)
5. [System Administrator \(Level 5\) Access](#)

For more information about account levels, see [Configuring MWTM User Account Levels \(Server Only\)](#), page 2-7.

User Passwords

The method that you use for setting user passwords depends on the type of authentication that you configure on the MWTM system (local or solaris).

Local Authentication

If *mwtm authtype* is set to *local*, the MWTM prompts you to:

- Enter the user password. When setting the password, follow the rules and considerations in [Creating Secure Passwords](#), page 2-7.
- Force the user to change the password at the next login. The default is to not force the user to change the password.

Whenever a user must change a password, the MWTM issues an appropriate message, and prompts for the user name and new password.

Solaris Authentication

If *mwtm authtype* is set to *solaris* or *linux*, users cannot change their passwords by using the MWTM client. Instead, they must manage their passwords on the external authentication servers by using Solaris or Linux commands, such as *passwd*.

All new passwords take effect the next time the MWTM automatically synchronizes local MWTM passwords with Solaris or Linux. You can manually synchronize passwords at any time by using the **mwtm syncusers** command. For more information, see [mwtm syncusers](#), page B-74.

Enabling Secure User Access

To enable secure user access for the MWTM:

Step 1 Log in to the MWTM server as the root user (see [Starting the MWTM Client, page 4-2.](#))

Step 2 To enable MWTM security, three prerequisites must be met:

- User access must be enabled.
- The authentication type must be set.
- Users must be added.

The **mwtm useraccess** enable command takes you through all three stages, checking the status of:

1. **mwtm useraccess**—Enabled or disabled.
2. **mwtm authtype**—If you have not already set the mwtm authentication type, you must do so now.
3. **mwtm adduser**—If you have already assigned users, the MWTM asks if you want to use the same user database, or create a new one. If you have not assigned users, you must do so now.



Tip For details on the **mwtm useraccess**, **mwtm authtype**, and **mwtm adduser** commands, see [Appendix B, “Command Reference.”](#)

Run the mwtm useraccess enable command:

```
cd /opt/CSC0sgm/bin
./mwtm useraccess enable
~text elided~
```

Step 3 To activate your security changes on the MWTM client, restart the MWTM server with the mwtm restart command (see [mwtm restart, page B-53.](#)) To activate your security changes on the MWTM web interface, clear the browser cache and restart the browser.

Use the remaining procedures in this chapter to further customize your MWTM security system.

Creating Secure Passwords

When setting passwords in the MWTM, the:

- Password must be at least 6 characters, up to 15 characters.
- Password cannot be identical to the user name.
- New password cannot be the same as the old password.
- MWTM does not allow users to switch back and forth between two passwords.
- Password cannot be a commonly used word. The MWTM server uses the system dictionary at */usr/share/lib/dict/words* (Solaris) or */usr/share/dict/words* (Linux) to determine whether a word is a commonly used word.

To use your own dictionary, add a line to the *System.properties* file:

- To disable the MWTM dictionary and allow common words, add:

```
DICT_FILE=/dev/null
```

- To use a custom dictionary, add:

```
DICT_FILE=/new-dictionary
```

where *new-dictionary* is the path and filename of the custom dictionary file, such as */users/usr11/words*. Each line in the custom dictionary must contain a single word, with no leading or trailing spaces.

Configuring MWTM User Account Levels (Server Only)

This section describes the user account levels, and the MWTM client and web interface actions that are available at each level:

- [Basic User \(Level 1\) Access, page 2-8](#)
- [Power User \(Level 2\) Access, page 2-8](#)
- [Network Operator \(Level 3\) Access, page 2-9](#)
- [Network Administrator \(Level 4\) Access, page 2-9](#)
- [System Administrator \(Level 5\) Access, page 2-11](#)

The account level that includes an action is the *lowest* level with access to that action. The action is also available to all higher account levels. For example, a System Administrator also has access to all Network Administrator actions.

Account levels are based on the action to be performed, not on the target network element. Therefore, if a user can perform an action on one MWTM network element (such as deleting a node), the user can perform the same action on all similar MWTM network elements (such as deleting an interface, signaling point, or linkset).



Note

Access to MWTM information and downloads on Cisco.com is already protected by Cisco.com, and is not protected by the MWTM.

To configure the account level for a user, use the **mwtm adduser** command, as described in [Implementing Secure User Access \(Server Only\)](#), page 2-2, or the **mwtm updateuser** or **mwtm newlevel** commands, as described in [Enabling and Changing Users and Passwords \(Server Only\)](#), page 2-14.

Basic User (Level 1) Access

Basic users can view MWTM data, load MWTM files, and use MWTM drill-down menus.

The following MWTM actions in the client and web interfaces are available to basic users:

MWTM Client Interface Actions

- Connecting to a new server
- Applying changes to views
- Loading the DEFAULT View and existing views, but not saving them
- Editing, loading, and applying preferences files, but not saving them
- Viewing and manipulating the topology map, and saving it as a JPEG, but not saving icon locations
- Viewing network elements, events, details, and notes
- Viewing the MWTM web interface Homepage
- Loading existing event filters, but not saving them
- Printing MWTM windows
- Launching CiscoWorks

MWTM Web Interface Actions

- Homepage
- Administrative page: System Information
- Administrative page: System Status
- Preferences
- Viewing Reports

Power User (Level 2) Access

The following MWTM actions in the client and web interfaces are available to power users:

MWTM Client Interface Actions

- Accessing all basic user client actions
- Editing network elements, events, and views
- Unignoring network elements and views
- Saving preferences files, event filters, and views
- Acknowledging events
- Viewing real-time data and graphs
- View, change and save event configuration, but no deployment of changes

MWTM Web Interface Actions

- Homepage
- Administrative page: System Information
- Administrative page: System Status
- Preferences

Network Operator (Level 3) Access

The following MWTM actions in the client and web interfaces are available to network operators:

MWTM Client Interface Actions

- Accessing all basic user and power user client actions
- Accessing Troubleshooting features
- Ignoring network elements and views
- Polling nodes
- Accessing the node through Telnet or SSH
- (ITP only) Viewing route table files and GTT files, but not editing them

MWTM Web Interface Actions

- Accessing all basic user and power user web actions
- Troubleshooting features
- Provisioning features
- Administrative page, all features

Network Administrator (Level 4) Access

The following MWTM actions in the client and web interfaces are available to network administrators:

MWTM Client Interface Actions

- Accessing all basic user, power user, and network operator client actions
- SNMP configuration
- Network discovery
- Deleting network elements
- Unmanaging nodes
- (ITP only) Editing and saving route table files, GTT files, and address table files
- (ITP only) Using the deployment wizard
- Enable and disable to generate reports (MSU Rates)

MWTM Web Interface Actions

- Accessing all basic user, power user, and network operator web actions
- Automatically logs into SSH terminal in enable mode (if enable password is set)

System Administrator (Level 5) Access

The following MWTM actions in the client and web interfaces are available to system administrators:

MWTM Client Interface Actions

- Accessing all basic user, power user, network operator, and network administrator client actions
- Managing nodes
- Accessing Trap Settings
- Deploying saved event configuration changes

MWTM Web Interface Actions

- Accessing all basic user, power user, network operator, and network administrator web actions
- Trap settings features

Automatically Disabling Users and Passwords (Server Only)

After you have implemented the basic MWTM security system, you can customize the system to automatically disable users and passwords when certain conditions are met (for example, a series of unsuccessful login attempts or a specified period of inactivity).



Tip

To view a list of current users and the status of user accounts, use the **mwtm listusers** command (see [mwtm listusers](#), page B-37).

To automatically disable users and passwords:

-
- Step 1** Log in to the MWTM server as the root or superuser:
- Root user—See [Becoming the Root User \(Server Only\)](#), page 4-2
 - Super user—See [Specifying a Super User \(Server Only\)](#), page 2-20
- Step 2** Enter the following command:
- ```
cd /opt/CSCOsgrm/bin
```
- Step 3** (Optional) To configure the MWTM to generate an alarm after a specified number of unsuccessful login attempts by a user, enter:
- ```
./mwtm badloginalarm number-of-attempts
```
- where *number-of-attempts* is the number of unsuccessful login attempts allowed before the MWTM generates an alarm.
- The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 5 unsuccessful attempts.
- To disable this action (that is, to prevent the MWTM from automatically generating an alarm after unsuccessful login attempts), enter:
- ```
./mwtm badloginalarm clear
```

- Step 4** (Optional) To configure the MWTM to disable a user's account automatically after a specified number of unsuccessful login attempts, enter:

```
./mwtm badlogindisable number-of-attempts
```

where *number-of-attempts* is the number of unsuccessful login attempts allowed before the MWTM disables the user's account. The MWTM does not delete the user from the user list, the MWTM only disables the user's account.

The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 10 unsuccessful attempts.

To re-enable the user's account, use the `mwtm enableuser` command.

To disable this action (that is, to prevent the MWTM from automatically disabling a user's account after unsuccessful login attempts), enter:

```
./mwtm badlogindisable clear
```

- Step 5** (Optional) The MWTM keeps track of the date and time each user last logged in. To configure the MWTM to disable a user's log in automatically after a specified number of days of inactivity, enter:

```
./mwtm inactiveuserdays number-of-days
```

where *number-of-days* is the number of days that a user can be inactive before the MWTM disables the user's account. The MWTM does not delete the user from the user list, the MWTM only disables the user's account.

The valid range is 1 day to an unlimited number of days. There is no default setting.

To re-enable the user's account, use the `mwtm enableuser` command.

This action is disabled by default. If you do not specify the `mwtm inactiveuserdays` command, user accounts are never disabled as a result of inactivity.

If you have enabled this action and you want to disable it (that is, to prevent the MWTM from automatically disabling user accounts as a result of inactivity), enter:

```
./mwtm inactiveuserdays clear
```

- Step 6** (Optional) If `mwtm authtype` is set to local, you can configure the MWTM to force users to change their passwords after a specified number of days.

To configure the MWTM to force users to change their passwords after a specified number of days, enter:

```
./mwtm passwordage number-of-days
```

where *number-of-days* is the number of days allowed before users must change their passwords.




---

**Note** You must have changed your password at least once for the `mwtm passwordage` command to properly age the password.

---

The valid range is 1 day to an unlimited number of days. There is no default setting.




---

**Note** The MWTM starts password aging at midnight on the day that you set the value. For example, if you use the `mwtm passwordage` command to set the password age to 1 day (24 hours), the password begins to age at midnight and expires 24 hours later.

---

This action is disabled by default. If you do not specify the `mwtm passwordage` command, users never need to change their passwords.



If you have enabled this action and you want to disable it (that is, prevent the MWTM from forcing users to change passwords), enter:

```
./mwtm passwordage clear
```



**Note** If mwtm authtype is set to solaris or linux, you cannot use the mwtm passwordage command. Instead, you must manage passwords on the external authentication servers.

**Step 7** (Optional) To configure the MWTM to automatically disconnect a client (this includes the MWTM client, the GTT editor, and the address table editor) after a specified number of minutes of inactivity, enter:

```
./mwtm clitimeout number-of-minutes
```

where *number-of-minutes* is the number of minutes a client can be inactive before the MWTM disconnects the client.

The valid range is 1 minute to an unlimited number of minutes. There is no default value.

This action is disabled by default. If you do not specify the mwtm clitimeout command, clients are never disconnected as a result of inactivity.

If you have enabled this action and you want to disable it (that is, never disconnect a client as a result of inactivity), enter the following command:

```
./mwtm clitimeout clear
```

## Manually Disabling Users and Passwords (Server Only)

As described in the [Automatically Disabling Users and Passwords \(Server Only\)](#), page 2-11, you can customize the MWTM to automatically disable users and passwords when certain conditions are met. However, you can also manually disable MWTM users and passwords whenever you suspect a security breach has occurred.

To disable MWTM users and passwords:

**Step 1** Login to the MWTM server as the root or superuser:

- Root user—See [Starting the MWTM Client](#), page 4-2
- Super user—See [Specifying a Super User \(Server Only\)](#), page 2-20

**Step 2** Enter:

```
cd /opt/CSCOsrgm/bin
```

**Step 3** (Optional) To delete a user entirely from the MWTM user access account list, enter:

```
./mwtm deluser username
```

where *username* is the name of the user.

If you later decide to add the user back to the account list, you must use the mwtm adduser command.

- Step 4** (Optional) If mwtm authtype is set to local, you can disable a user's password. To disable a user's password, enter:

```
./mwtm disablepass username
```

where *username* is the name of the user. The MWTM does not delete the user from the account list, the MWTM only disables the user's password.



---

**Note** If mwtm authtype is set to solaris or linux, you cannot use the mwtm disablepass command. Instead, you must manage passwords on the external authentication servers.

---

The user must change the password the next time he or she logs in.

You can also re-enable the user's account with the same password, or with a new password:

- To re-enable the user's account with the same password as before, use the mwtm enableuser command.
- To re-enable the user's account with a new password, use the mwtm userpass command.

- Step 5** (Optional) To disable a user's account, but not the user's password, enter:

```
./mwtm disableuser username
```

where *username* is the name of the user.



---

**Note** If mwtm authtype is set to solaris or linux, you must be logged in as the root user, not as a superuser, to enter this command.

---

The MWTM does not delete the user from the account list; the MWTM only disables the user's account. The user cannot log in until you re-enable the user's account:

- To re-enable the user's account with the same password as before, use the mwtm enableuser command.
  - To re-enable the user's account with a new password, use the mwtm userpass command.
- 

## Enabling and Changing Users and Passwords (Server Only)

Of course, the MWTM also enables you to re-enable users and passwords, and change user accounts. To enable and change users and passwords, use the following procedures:

- 
- Step 1** Log in to the MWTM server as the root or superuser:
- Root user—See [Starting the MWTM Client, page 4-2](#)
  - Super user—See [Specifying a Super User \(Server Only\), page 2-20](#)
- Step 2** Enter the following command:
- ```
# cd /opt/CSC0sgm/bin
```

- Step 3** (Optional) To re-enable a user's account, which had been disabled either automatically by the MWTM or by a superuser, enter the following command:

```
# ./mwtm enableuser username
```

where *username* is the name of the user. The MWTM re-enables the user's account with the same password as before.



Note If mwtm authtype is set to solaris or linux, you must be logged in as the root user, not as a superuser, to enter this command.

- Step 4** (Optional) If mwtm authtype is set to local, you can change a user's password, or re-enable the user's account with a new password, if the user's account had been disabled either automatically by the MWTM or by a superuser. To change a password or to re-enable a user's account with a new password, enter:

```
# ./mwtm userpass username
```

where *username* is the name of the user.

The MWTM prompts you for the new password. When setting the password, follow the rules and considerations in the [Creating Secure Passwords, page 2-7](#).

If the user's account has also been disabled, the MWTM re-enables the user's account with the new password.



Note If mwtm authtype is set to solaris or linux, you cannot use the mwtm userpass command. Instead, you must manage passwords on the external authentication servers.

- Step 5** (Optional) To change a user's account level and password, enter the following command:

```
# ./mwtm updateuser username
```

where *username* is the name of the user.



Note If mwtm authtype is set to solaris or linux, you must be logged in as the root user, not as a superuser, to enter this command.

The MWTM prompts you for the new account level. Valid levels are described in [User Levels, page 2-4](#):

If mwtm authtype is set to local, the MWTM also prompts you for the user's new password. When setting the password, follow the rules and considerations in [Creating Secure Passwords, page 2-7](#).

- Step 6** (Optional) To change a user's account level, but not the user's password, enter the following command:

```
# ./mwtm newlevel username
```

where *username* is the name of the user.

The MWTM prompts you for the new account level. Valid levels are described in [User Levels, page 2-4](#).

Displaying a Message of the Day (Server Only)

You can use the MWTM to display a user-specified MWTM system notice called the message of the day. You can use the message of the day to inform users of important changes or events in the MWTM system. The message of the day also gives users an opportunity to exit the MWTM client, Event Editor, GTT Editor (ITP only), or Address Table Editor (ITP only) before starting them.

If you enable the message of the day, it appears whenever a user attempts to launch a client. If the user accepts the message, the client launches. If the user declines the message, the client does not launch.

To display the Message of the Day dialog, use one of the following procedures:

- Launch a client. If there is a message of the day, the Message of the Day dialog appears.
- Choose **View > Message of the Day** from the MWTM main menu.
- Select the MWTM server name in the lower-right corner of the MWTM main window.

The Message of the Day dialog contains the following fields:

Field or Button	Description
Message of the Day Last Updated	Date and time the message of the day was last updated. If there is no message of the day, the MWTM displays Unknown.
Message Field	Text of the message of the day. If there is no message of the day, the MWTM displays <i>There is no message of the day.</i>
Accept	Closes the Message of the Day dialog and launches the client. If you do not click Accept, you cannot launch the client. This button is available when there is a message of the day and you launch a client.
Decline	Closes the Message of the Day dialog and exits the client. This button is available when there is a message of the day and you launch a client.
OK	Closes the Message of the Day dialog without exiting the client. This button is available if you displayed the Message of the Day dialog by choosing View > Message of the Day from the MWTM main menu.

To configure the MWTM to display a message of the day:

-
- Step 1** Log in to the MWTM server as the root or superuser:
- Root user—See [Starting the MWTM Client, page 4-2](#)
 - Super user—See [Specifying a Super User \(Server Only\), page 2-20](#)

- Step 2** Enter the following commands:

```
cd /opt/CSCosgm/bin
./mwtm motd enable
```

The MWTM displays:

```
Enter location of the message of the day file: [/opt/CSCosgm/etc/motd]
```

Step 3 To accept the default value, press **Enter**; or type a different location and press **Enter**.

The MWTM displays:

```
Setting Message of the Day File to: [/opt/CSCOsgrm/etc/motd]
Message of the Day File set to: [/opt/CSCOsgrm/etc/motd]
MWTM server must be restarted for changes to take effect.
```

Step 4 To create the message text (the first time) or edit the existing text, enter:

```
./mwtm motd edit
```

Step 5 To display the contents of the message of the day file, enter:

```
./mwtm motd cat
```

Step 6 To disable the message of the day file, enter:

```
./mwtm motd disable
```

Manually Synchronizing Local MWTM Passwords (Server Only)

If mwtm authtype is set to solaris or linux, the MWTM automatically synchronizes local MWTM passwords with the operating system at 1:30 AM each night (this setting can be changed using the root crontab). However, you can also manually synchronize passwords at any time.

To manually synchronize local MWTM passwords:

Step 1 Log in to the MWTM server as the root or superuser:

- Root user—See [Starting the MWTM Client, page 4-2](#)
- Super user—See [Specifying a Super User \(Server Only\), page 2-20](#)

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOsgrm/bin
```

Step 3 Synchronize the MWTM passwords:

```
./mwtm syncusers
```

The MWTM synchronizes the passwords with solaris.

Listing All Currently Defined Users (Server Only)

To list all currently defined users in the MWTM User-Based Access account list:

-
- Step 1** Log in to the MWTM server as the root or superuser:
- Root user—See [Starting the MWTM Client, page 4-2](#)
 - Super user—See [Specifying a Super User \(Server Only\), page 2-20](#)
- Step 2** Change to the */bin* directory:
- ```
cd /opt/CSCOsgm/bin
```
- Step 3** List all users:
- ```
./mwtm listusers
```
- The MWTM displays the following information for each user:
- User name
 - Last time the user logged in
 - User's account access level
 - User's current account status, such as Account Enabled or Password Disabled
- Step 4** To list information for a specific user, enter:
- ```
./mwtm listusers username
```

where *username* is the name of the user.



---

**Note** You can also view user account information on the MWTM User Accounts web page. For more information, see [Viewing User Accounts, page 11-21](#).

---

## Displaying the Contents of the System Security Log (Server Only)

To display the contents of the system security log with PAGER:

- 
- Step 1** Log in to the MWTM server as the root or superuser:
- Root user—See [Starting the MWTM Client, page 4-2](#)
  - Super user—See [Specifying a Super User \(Server Only\), page 2-20](#)
- Step 2** Change to the */bin* directory:
- ```
cd /opt/CSCOsgm/bin
```

Step 3 Display the security log contents:

```
./mwtm seclog
```

The following security events are recorded in the log:

- All changes to system security, including adding users
- Login attempts, whether successful or unsuccessful, and logoffs
- Attempts to switch to another user's account, whether successful or unsuccessful
- Attempts to access files or resources of higher account level
- Access to all privileged files and processes
- Operating system configuration changes and program changes, at the Solaris level
- MWTM restarts
- Failures of computers, programs, communications, and operations, at the Solaris level

Step 4 To clear the log, enter:

```
./mwtm seclog clear
```

The default path and filename for the system security log file is */opt/CSCOs/gm/logs/sgmSecurityLog.txt*. If you installed the MWTM in a directory other than */opt*, then the system security log file is located in that directory.



Note

You can also view the system security log on the MWTM System Security Log web page. For more information, see [Viewing the Security Log, page 11-23](#).

Restoring Security-Related MWTM Data (Server Only)

If you inadvertently delete your user accounts, or make other unwanted changes to your MWTM security information, the MWTM can restore the security-related parts of the MWTM data files from the previous night's backup.

To restore the security-related MWTM data files:

Step 1 Log in as the root user (for details see [Starting the MWTM Client, page 4-2](#)).

Step 2 Change to the */bin* directory:

```
cd /opt/CSCOs/gm/bin
```

Step 3 Restore the security-related data:

```
./mwtm restore security
```

The MWTM restores the data.

Disabling MWTM User-Based Access (Server Only)

To completely disable MWTM User-Based Access:

-
- Step 1** Log in to the MWTM server as the root or superuser:
- Root user—See [Starting the MWTM Client, page 4-2](#)
 - Super user—See [Specifying a Super User \(Server Only\), page 2-20](#)
- Step 2** Change to the `/bin` directory:
- ```
cd /opt/CSCOsgm/bin
```
- Step 3** Disable user-based access:
- ```
./mwtm useraccess disable
```

The MWTM user access is disabled the next time you restart the MWTM server (using the `mwtm restart` command).

Specifying a Super User (Server Only)

You can use the MWTM to specify a *superuser*. A superuser can perform most actions that otherwise require the user to be logged in as the root user. (The root user can still perform those actions, too.) If you specify a superuser, the server also runs as the superuser and not as the root user.



Caution

As a superuser, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are a relatively inexperienced UNIX user, limit your activities as a superuser to the tasks described in this document.

When you specify a superuser, remember that:

- The user must exist in the local `/etc/passwd` file. You cannot specify a user that is defined in a distributed Network Information Services (NIS) system.
- The superuser does not have access to all MWTM commands; you must still be logged in as the root user to enter certain commands. You must still be logged in as the root user to enter the following commands:
 - `mwtm authtype`
 - `mwtm backup`
 - `mwtm backupdir`
 - `mwtm browserpath`
 - `mwtm certgui`
 - `mwtm certtool`
 - `mwtm clean`
 - `mwtm cleanall`
 - `mwtm cleandb`
 - `mwtm cwsetup`

- mwtm evilstop
 - mwtm jspport
 - mwtm keytool
 - mwtm killclients
 - mwtm reboot
 - mwtm restore
 - mwtm restoreprops
 - mwtm setpath, if you are specifying a *username*
 - mwtm sounddir
 - mwtm ssl
 - mwtm stopclients
 - mwtm superuser
 - mwtm syncusers
 - mwtm termproxy
 - mwtm trapsetup
 - mwtm uninstall
 - mwtm webport
 - mwtm xtermpath
- If the mwtm authtype is set to solaris or linux, you must still be logged in as the root user to enter the following commands:
 - mwtm adduser
 - mwtm disablepass
 - mwtm passwordage
 - mwtm updateuser
 - mwtm userpass
- If the SNMP trap port number on the MWTM server is less than 1024, you cannot use the mwtm superuser command. To correct this situation, you must specify a new SNMP trap port number that is greater than 1024:
 - To change the SNMP trap port number in the nodes in your network, use the snmp-server host command. By default, the MWTM listens for traps from trap multiplexing nodes and NMS applications on port 44750, so that is a good port number to choose. The SNMP trap port number must be the same on all nodes in your network.
 - For more information, see the description of the snmp-server host command in the “Node Requirements” section of the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.
 - Use the mwtm trapsetup command to change the SNMP trap port number in the MWTM server to match the port number in the nodes in your network. For more information, see [mwtm trapsetup](#), page B-76.

To specify a superuser on the MWTM server:

Step 1 Log in as the root user (see [Becoming the Root User \(Server Only\)](#), page 4-2).

Step 2 Change to the `/bin` directory:

```
cd /opt/CSCosgm/bin
```

Step 3 Specify the superuser:

```
./mwtm superuser username
```

where *username* is the name of the user.

Implementing SSL Support in the MWTM



Note

If you chose the Solaris or Linux authentication options (during installation or through the `mwtm authtype` command) you must enable SSL. For details on the `mwtm authtype` command, see [mwtm authtype](#), page B-8.

You can implement Secure Sockets Layer (SSL) support in your MWTM system. When you do, the MWTM uses secure sockets to encrypt all communication between the MWTM clients and server.

This section includes the following information:

- [Enabling SSL Support on the MWTM Server](#), page 2-22
- [Downloading the MWTM SSL Module for Windows Using the Web Interface](#), page 2-24
- [Downloading the Self-Signed SSL Certificate from the MWTM Server](#), page 2-26
- [Launching the MWTM Certificate Tool for SSL](#), page 2-26
- [Exporting an SSL Certificate](#), page 2-28
- [Viewing Detailed Information About a SSL Certificate](#), page 2-29
- [Managing SSL Support in the MWTM](#), page 2-30
- [Disabling SSL Support in the MWTM](#), page 2-30

Enabling SSL Support on the MWTM Server

To enable SSL support in the MWTM, perform the following:

Step 1 Install an SSL key/certificate pair in the MWTM by using one of the following procedures:

- To install a new SSL key and a self-signed certificate, generate the key and certificate by logging in as the root user on the MWTM server and entering the **`mwtm keytool genkey`** command.

The MWTM stops the MWTM server and these prompts appear:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
```

```
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Enter the requested information.

The MWTM generates the following files:

- `/opt/CSCOSgm/etc/ssl/server.key` is the MWTM server's private key. Ensure that unauthorized personnel cannot access this key.
 - `/opt/CSCOSgm/etc/ssl/server.crt` is the self-signed SSL certificate.
 - `/opt/CSCOSgm/etc/ssl/server.csr` is a certificate signing request (CSR). It is not used if you are using a self-signed SSL certificate.
- To install a new SSL key and a certificate signed by a certificate authority (CA), generate the key and a CSR by logging in as the root user on the MWTM server and entering the **mwtm keytool genkey** command.

The MWTM stops the MWTM server and issues the following prompts:

```
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (your hostname) []:
Email Address []:
Certificate Validity (number of days)? [min: 30, default: 365]
```

Enter the requested information.

The MWTM generates the following files:

- `/opt/CSCOSgm/etc/ssl/server.key` is the MWTM server's private key. Ensure that unauthorized personnel cannot access this key.
- `/opt/CSCOSgm/etc/ssl/server.csr` is a CSR.
- `/opt/CSCOSgm/etc/ssl/server.crt` is the self-signed SSL certificate. It is not used if you are using a CA-signed SSL certificate; the CA-signed certificate overrides the self-signed certificate.

Print the CSR in X.509 format, by logging in as the root user on the MWTM server and entering the **mwtm keytool print_csr** command.

Send the CSR to a CA to be signed.

After the CA signs the certificate, log in as the root user on the MWTM server and enter the following command:

```
./mwtm keytool import_cert cert_filename
```

where *cert_filename* is the name of the signed certificate.

The MWTM stops the MWTM server and imports the certificate in X.509 format.

- To use an existing signed key/certificate pair, log in as the root user on the MWTM server and enter the following command:

```
./mwtm keytool import_key key_filename cert_filename
```

where *key_filename* is the name of the existing SSL key and *cert_filename* is the name of the existing signed certificate.

The MWTM stops the MWTM server and imports the SSL key in OpenSSL format and the signed SSL certificate in X.509 format.

- Step 2** Enable SSL support in the MWTM, by logging in as the root user on the MWTM server and entering the **mwtm ssl enable** command.
- Step 3** Restart the MWTM server.
- Step 4** Set up the MWTM client-side SSL certificate trust relationship, by downloading and importing the self-signed or CA-signed certificate on every remote MWTM client, Windows as well as Solaris, that connects to the MWTM server.
 - a. (Self-signed certificate only) Download the self-signed certificate (*server.crt*) by using the procedure in [Downloading the Self-Signed SSL Certificate from the MWTM Server, page 2-26](#).
 - b. Import the self-signed or CA-signed certificate by using the procedure in [Launching the MWTM Certificate Tool for SSL, page 2-26](#).
- Step 5** Restart the MWTM client.

The MWTM clients can now connect to the MWTM server by using SSL. All communication between the server and clients is encrypted.

If an MWTM client, GTT editor (ITP only), or Address Table editor (ITP only) that is not SSL-enabled attempts to connect to an SSL-enabled MWTM server, the MWTM displays an appropriate warning message and opens the MWTM Client for Windows page. You can then download and install a new MWTM SSL module for the client to use to connect to that MWTM server.

If the client is SSL-enabled but does not have the correct certificate, the MWTM displays an appropriate warning message and opens the MWTM Server SSL Certificate page. You can then download the signed SSL certificate in X.509 format to the client.

Downloading the MWTM SSL Module for Windows Using the Web Interface

To install the MWTM SSL module on a Windows system from the MWTM web interface:

- Step 1** From your browser, go to the URL for the MWTM Homepage:
`http://your_mwtm_server:1774`
 where *your_mwtm_server* is the name or IP address of the MWTM server and *1774* is the web port being used by the MWTM (1774 is the default port number.) If you do not know the name or web port of the MWTM server, contact the system administrator who installed the MWTM server software.
 The MWTM web interface home page appears.
- Step 2** Click **Download Windows Client**. Ensure that your browser is pointed to an MWTM, SSL-enabled server.
- Step 3** Right-click **Download SSL Module for MWTM Client on Windows XP**. Choose the **Save Link As** or **Save Target As** option.



Note If you are using Internet Explorer, change the *.zip* extension to *.jar* during the Save Target As option.

- Step 4** When queried, save the file under *<Installed Drive>:\Program Files\Cisco Systems\MWTMClient\lib* where *<Installed Drive>* is the disk on which the MWTM client is installed.
- Step 5** You are prompted to launch the client, then download the self-signed SSL certificate (follow the subsequent procedures).
-

Downloading the Self-Signed SSL Certificate from the MWTM Server

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can download the MWTM server's signed SSL certificate to all remote MWTM clients that connect to the server using SSL.

To download the certificate from the MWTM Server SSL Certificate page, use the following procedure on each remote MWTM client:

-
- Step 1** In a web browser, enter the following URL:
- ```
https://server_name:1774
```
- where *server\_name* is the name or IP address of the server on which the MWTM server is running and *1774* is the Web port being using by the MWTM (**1774** is the default port number.) If you do not know the name or Web port of the MWTM server, contact the system administrator who installed the MWTM server software.
- The Server SSL Certificate page appears.
- Step 2** Right-click **Download Server SSL Certificate**.
- Step 3** Select **Save Link As** (or **Save Target As**) from the right-click menu.
- Step 4** Select a directory in which to save the certificate (*server.crt*), and click **Save**. The MWTM downloads the *server.crt* file into the specified directory.
- 

## Launching the MWTM Certificate Tool for SSL

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can launch the MWTM Certificate Tool for SSL. The MWTM Certificate Tool dialog box lists all SSL certificates that the MWTM client imported. In this dialog box, you specify whether to import, export, and display detailed information about SSL certificates.

To launch the MWTM SSL Certificate Tool, use one of the following procedures:

- In Solaris, log in as the root user and enter the following commands:

```
cd /opt/CSCosgm/bin
./mwtm certgui
```

For more information, see [mwtm certgui](#), page B-12.
- In Windows, choose **Start > Programs > Cisco MWTM Client > MWTM SSL Certificate Tool**.

The MWTM displays the MWTM Certificate Tool dialog box.

For each SSL certificate, the MWTM Certificate Tool dialog box displays:

| Field or Button | Description                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Issued to       | Host name of the MWTM server to which the SSL certificate was issued.                                                                 |
| Issued by       | Certificate authority (CA) that issued the SSL certificate.<br>Self-signed SSL certificates display the host name of the MWTM server. |
| Expiration Date | Date on which the SSL certificate expires.                                                                                            |

| Field or Button | Description                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Import          | Displays the Open dialog box for an SSL certificate, which you use to import SSL certificates (for details, see <a href="#">Importing an SSL Certificate to an MWTM Client, page 2-27</a> ). |
| Export          | Displays the Save dialog box for an SSL certificate, which you use to export the selected SSL certificate.                                                                                   |
| Remove          | Removes the selected SSL certificate from the table.                                                                                                                                         |
| Details         | Displays the Certificate Information dialog box, which provides detailed information about the selected certificate.                                                                         |
| Exit            | Closes the MWTM Certificate Tool dialog box.                                                                                                                                                 |
| Help            | Displays online help for the current window.                                                                                                                                                 |

## Importing an SSL Certificate to an MWTM Client

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can import the MWTM server's self-signed SSL certificate, or a CA-signed SSL certificate, to all remote MWTM clients that connect to the server using SSL.



### Note

If you are using a Solaris client, you can import by using the MWTM SSL Certificate Tool as described in this section, or the CLI command `mwtm certtool` (for details, see [mwtm certtool, page B-12](#)). If you are using a Windows client, you must use the MWTM SSL Certificate Tool.

To import an SSL certificate, launch the MWTM SSL Certificate Tool, as described in [Launching the MWTM Certificate Tool for SSL, page 2-26](#), then click **Import**. The MWTM displays the Open dialog box for SSL certificates.

Use the Open dialog box to locate the SSL certificate that you want to import. The Open dialog box contains:

| Field or Button                                                                                  | Description                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Look In                                                                                          | Click to select the directory in which you want to find the SSL certificate. Accept the default directory, or select a new directory from the drop-down list box.<br><br>For a self-signed certificate, locate the directory in which you downloaded the certificate. |
| File Name                                                                                        | Enter a name for the SSL certificate, or select a file from those listed in the "Open" field. The MWTM displays the name of the certificate in the "File Name" field.                                                                                                 |
| Files of Type                                                                                    | Specifies the type of file to display, and displays all files of that type in the selected directory. For SSL certificates, this field displays "All files," which means files of all types appear in the table.                                                      |
|  Up One Level | Displays the subfolders and files that are in the folder that is up one level from the currently visible folder.                                                                                                                                                      |
|  Desktop      | Displays the subfolders and files that are on your workstation desktop.                                                                                                                                                                                               |

| Field or Button                                                                                     | Description                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  Create New Folder | Creates a new subfolder in the visible folder.                                                                                                                  |
|  List              | Displays only icons for subfolders and files.                                                                                                                   |
|  Details           | Displays detailed information for subfolders and files, including their size, type, date they were last modified, and so on.                                    |
| Open                                                                                                | Imports the file, closes the Open dialog box for an SSL certificate, and populates the MWTM Certificate Tool dialog box with the SSL certificate's information. |
| Cancel                                                                                              | Closes the Open dialog box for an SSL certificate without importing the file.                                                                                   |

## Exporting an SSL Certificate

If you have implemented Secure Sockets Layer (SSL) support in your MWTM system, you can export SSL certificates that have been imported to the MWTM client.

To export a SSL certificate, launch the MWTM SSL Certificate Tool, as described in [Launching the MWTM Certificate Tool for SSL, page 2-26](#), select a certificate from the list, then click **Export**. The MWTM displays the Save dialog for SSL certificates.

Use the Save dialog box to export the SSL certificate to another directory. The Save dialog box contains:

| Field or Button                                                                                       | Description                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Save In                                                                                               | Click to select the directory in which you want to save the SSL certificate. Accept the default directory, or select a new directory from the drop-down list box.<br><br>For a self-signed certificate, locate the directory in which you downloaded the certificate. |
| File Name                                                                                             | Enter a name for the SSL certificate, or select a file from those listed in the "Save In" field. The MWTM displays the name of the certificate in the "File Name" field.                                                                                              |
| Files of Type                                                                                         | Specifies the type of file to save, and displays all files of that type in the selected directory. For SSL certificates, this field displays "All files," which means files of all types.                                                                             |
|  Up One Level      | Displays the subfolders and files that are in the folder that is up one level from the currently visible folder.                                                                                                                                                      |
|  Desktop           | Displays the subfolders and files that are on your workstation desktop.                                                                                                                                                                                               |
|  Create New Folder | Creates a new subfolder in the visible folder.                                                                                                                                                                                                                        |
|  List              | Displays only icons for subfolders and files.                                                                                                                                                                                                                         |



| Field or Button                                                                           | Description                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  Details | Displays detailed information for subfolders and files, including their size, type, date they were last modified, and so on.                                                                                                                        |
| Save                                                                                      | Saves the file, closes the Save dialog box for an SSL certificate, and returns to the MWTM Certificate Tool dialog box. Click <b>Exit</b> to close the MWTM Certificate Tool dialog box and export the self-signed SSL certificate in X.509 format. |
| Cancel                                                                                    | Closes the Save dialog for an SSL certificate without saving the file.                                                                                                                                                                              |

**Related Topics:**

[Launching the MWTM Certificate Tool for SSL, page 2-26](#)

## Viewing Detailed Information About a SSL Certificate

If you implemented Secure Sockets Layer (SSL) support in your MWTM system, you can view detailed information about SSL certificates that were imported to the MWTM client.

To view detailed information about an SSL certificate, use one of the following procedures:

- Click the locked padlock icon in the lower-left corner of any MWTM window.
- Launch the MWTM SSL Certificate Tool, as described in [Launching the MWTM Certificate Tool for SSL, page 2-26](#), select an SSL certificate from the list and click **Details**.

The MWTM displays the Certificate Information dialog.

For the selected SSL, the Certificate Information dialog box displays:

| Field or Button     | Description                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Subject             | Node to which the SSL certificate was issued.<br><br>This field always includes the Common Name (CN) of the subject, which must match the fully qualified host name of your MWTM server, such as <i>xxxx.company.com</i> .<br><br>This field might also contain other information, such as the Country (C), Organizational Unit (OU), or Organization (O) of the subject. |
| Issuer              | CA that issued the SSL certificate.<br><br>This field might include the Common Name (CN) of the issuer, as well as the Country (C), Organizational Unit (OU), or Organization (O) of the issuer.                                                                                                                                                                          |
| Version             | Version of the SSL certificate, such as “V1.”                                                                                                                                                                                                                                                                                                                             |
| Serial number       | Serial number associated with the SSL certificate.                                                                                                                                                                                                                                                                                                                        |
| Signature algorithm | Asymmetric algorithm ensures that the digital signature is secure, such as “MD5withRSA.”                                                                                                                                                                                                                                                                                  |
| Valid from          | Date and time on which the SSL certificate was created or became valid.                                                                                                                                                                                                                                                                                                   |
| Valid to            | Date and time on which the SSL certificate expires.                                                                                                                                                                                                                                                                                                                       |

| Field or Button | Description                                                                                                                                                                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Public key      | Public key associated with the SSL certificate, used for encryption and for verifying signatures.                                                                                                                                                  |
| OK              | Closes the Certificate Information dialog box.<br><br>When you are ready to close the dialog box, click <b>OK</b> . The MWTM closes the Certificate Information dialog. If necessary, click <b>Exit</b> to close the MWTM Certificate Tool dialog. |

**Related Topics:**

[Launching the MWTM Certificate Tool for SSL, page 2-26](#)

## Managing SSL Support in the MWTM

You use the MWTM to manage SSL support. To:

- Display the current status of SSL support in the MWTM, including whether SSL support is enabled or disabled and which SSL keys and certificates exist, use either the `mwtm ssl status` or `mwtm sslstatus` command.
- Print the MWTM server's SSL certificate in X.509 format, use the `mwtm keytool print_crt` command.
- List the SSL key/certificate pair on the MWTM server, use the `mwtm keytool list` command.
- List all SSL certificates on the MWTM client, launch the MWTM SSL Certificate Tool. The MWTM lists each imported certificate, including to whom the certificate was issued, who issued the certificate, and when the certificate expires.

For more information on the use of these commands, see [Appendix B, "Command Reference"](#)

For more information on launching the MWTM SSL Certificate Tool, see [Exporting an SSL Certificate, page 2-28](#).

## Disabling SSL Support in the MWTM

You use the MWTM to disable SSL support in the MWTM, and to remove SSL keys and certificates from the MWTM server and clients. To:

- Disable SSL support in the MWTM, use the `mwtm ssl disable` command.  
For more information, see [mwtm ssl, page B-70](#).
- Remove all SSL keys and certificates from the MWTM server, use the `mwtm keytool clear` command. The MWTM stops the MWTM server, if necessary, and removes the keys and certificates. Before restarting the server, you must generate new SSL keys by using the `mwtm keytool genkey` command, or you must completely disable SSL using the `mwtm ssl disable` command.

For more information on the use of these commands, see [Appendix B, "Command Reference"](#).

- Remove an SSL certificate from the MWTM client, launch the MWTM SSL Certificate Tool. The MWTM lists each imported certificate. Select the certificate that you want to remove, and click **Remove**. The MWTM deletes the certificate from the list.

For more information on launching the MWTM SSL Certificate Tool, see [Exporting an SSL Certificate, page 2-28](#).

# Limiting MWTM Client Access to the MWTM Server (Server Only)

By default, when you first install the MWTM, all MWTM client IP addresses can connect to the MWTM server. However, you use the MWTM to limit client access to the server by creating and maintaining the *ipaccess.conf* file.

You can create the *ipaccess.conf* file and populate it with a list of MWTM client IP addresses that can connect to the MWTM server. The MWTM allows connections from only those clients, plus the local host. If the file exists but is empty, the MWTM allows connections only from the local host. (The MWTM always allows connections from the local host.)

When you first install the MWTM, the *ipaccess.conf* file does not exist and the MWTM allows all client IP addresses to connect to the MWTM server. To create the *ipaccess.conf* file and work with the list of allowed client IP addresses:

- 
- Step 1** Log in to the MWTM server as the root or superuser:
- Root user—See [Becoming the Root User \(Server Only\)](#), page 4-2
  - Super user—See [Specifying a Super User \(Server Only\)](#), page 2-20
- Step 2** Change to the bin directory:
- ```
cd /opt/CSCOsgrm/bin
```
- Step 3** Create the *ipaccess.conf* file:
- To create the *ipaccess.conf* file and add a client IP address to the list, enter:

```
./mwtm ipaccess add
```
 - To create the *ipaccess.conf* file and open the file to edit it directly, enter:

```
./mwtm ipaccess edit
```

The default directory for the file is located in the MWTM installation directory:

- If you installed the MWTM in the default directory, */opt*, then the default directory is */opt/CSCOsgrm/etc*.
- If you installed the MWTM in a different directory, then the default directory is located in that directory.

In the *ipaccess.conf* file, begin all comment lines with a pound sign (#).

All other lines in the file are MWTM client IP addresses, with one address per line.

Wildcards (*) are allowed, as are ranges (for example, 1-100). For example, if you input the address *.*.*. then all clients can connect to the MWTM server.

After you create the *ipaccess.conf* file, you can use the full set of mwtm ipaccess keywords to work with the file:

- **clear**—Remove all client IP addresses from the *ipaccess.conf* file, and allow connections from any MWTM client IP address.
- **list**—List all client IP addresses currently in the *ipaccess.conf* file. If no client IP addresses are listed (that is, the list is empty), connections from any MWTM client IP address are allowed.
- **rem**—Remove the specified client IP address from the *ipaccess.conf* file.
- **sample**—Print out a sample *ipaccess.conf* file.

For more information, see [mwtm ipaccess, page B-35](#).

Any changes you make to the *ipaccess.conf* file take effect when you restart the MWTM server.

You can also use the MWTM to limit the IP addresses that can send traps to the server by creating and maintaining the *trapaccess.conf* file. For more information, see the “[Limiting Traps by IP Address](#)” section on [page 3-9](#).

Backing Up or Restoring MWTM Files (Server Only)

The MWTM automatically backs up all MWTM data files to the MWTM installation directory daily at 1:30 AM.

To change the time at which the MWTM automatically backs up files, log in as the root user and change the *root crontab* file:

- **crontab -l** lists cron jobs.
- **crontab -e** opens up an editor so you can make changes and save them.



Note

The MWTM performs a database integrity check during the backup. If the check fails, the previous backup is not be overwritten, and the MWTM creates a new failed file (for example: *mwtm61-server-backup-failed.tar.Z*).

This section contains these topics:

- [Backing Up MWTM Data Files, page 2-32](#)
- [Changing the Backup Directory, page 2-33](#)
- [Setting the Number of Backup Days, page 2-33](#)
- [Restoring the MWTM Data Files, page 2-34](#)

Backing Up MWTM Data Files

To manually back up the MWTM data files at any time on a Solaris or Linux server:

Step 1 Log in as the root user. See [Becoming the Root User \(Server Only\), page 4-2](#).

Step 2 Change to the bin directory:

```
cd /opt/CSCosgm/bin
```

Step 3 Back up the MWTM files:

```
./mwtm backup
```

The MWTM backs up the data files in the installation directory.

If you installed the MWTM in the default directory, */opt*, then the default backup directory is also */opt*. If you installed the MWTM in a different directory, then the default backup directory is that directory.

Changing the Backup Directory

To change the directory in which the MWTM stores its nightly backup files:

Step 1 Log in as the root user. See [Becoming the Root User \(Server Only\)](#), page 4-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgrm/bin
```

Step 3 Change the backup directory location:

```
./mwtm backupdir directory
```

where *directory* is the new backup directory.

If the new directory does not exist, the MWTM does not change the directory, but issues an appropriate warning message.

Setting the Number of Backup Days

To set the number of days that the MWTM saves backup files:

Step 1 Log in as the root user. See [Becoming the Root User \(Server Only\)](#), page 4-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgrm/bin
```

Step 3 Change the number of backup days (default is 1):

```
./mwtm backupdays
```

```
Current value is: 1
```

```
Enter number of days to save backup files (1-30): [1]
```

Step 4 Enter a value for the number of days from 1 to 30. For example:

```
Enter number of days to save backup files (1-30): [1] 5
```

```
Setting number of days to save backup files to 5 days.
```

The MWTM will save backup files for the number of days that you entered. In this example, the MWTM saves backup files for the last five days, and deletes backup files that are older than five days.

Restoring the MWTM Data Files

You can restore data files on the same Solaris or Linux server, or on a different Solaris or Linux server running the MWTM 6.1.

To restore the MWTM data files from a previous backup:

Step 1 Log in as the root user. See [Becoming the Root User \(Server Only\)](#), page 4-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCosgm/bin
```

Step 3 Restore the MWTM data files:

```
./mwtm restore
```

The MWTM restores the data files.



Note

If the number of backup days has been set to more than one day (see [Setting the Number of Backup Days](#), page 2-33), the MWTM will prompt you for a server or client backup file to restore from (because there would be more than one backup file to choose from).



Warning

Do not interrupt this command. Doing so can corrupt your MWTM data files.

The **mwtm restore** command provides optional keywords that you use to restore only selected MWTM data files, such as GTT files (ITP only), route table files (ITP only), log files, report files, or security files. For more information, see [mwtm restore](#), page B-54.

Removing MWTM Data from the MWTM Server

If you ever want to remove all MWTM data from the MWTM server without uninstalling the product, you can do so in one of two ways. Both ways restore the MWTM server to a state that would exist after a new installation of the MWTM.

Method 1

To remove all MWTM data from the MWTM server, *excluding* message log files, backup files, and report files:

Step 1 Log in as the root user (see [Becoming the Root User \(Server Only\)](#), page 4-2).

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgrm/bin
```

Step 3 Remove the MWTM data:

```
./mwrm clean
```

Data removed includes all MWTM data, notes, preferences, security settings, route files (ITP only), GTT files (ITP only), address table files (ITP only), seed files, event filters, report control files, and views, as well as any user-created files stored in the MWTM directories.

Method 2

To remove all MWTM data from the MWTM server, including all view files, notes that are associated with network elements, and event filters and preferences, *excluding* message log files, backup files, report files, configuration settings, and security settings:

Step 1 Log in as the root user. See [Becoming the Root User \(Server Only\)](#), page 4-2.

Step 2 Change to the bin directory:

```
cd /opt/CSCOsgrm/bin
```

Step 3 Enter:

```
# ./mwrm cleandb
```

This command restores the MWTM server to a state that would exist after a new installation of the MWTM, except for the presence of the retained files. Data removed includes all MWTM data, notes, preferences, route files (ITP only), GTT files (ITP only), address table files (ITP only) and views, as well as any user-created files stored in the MWTM directories.

To remove all MWTM data from the MWTM server, **including** message log files, backup files, and report files, log in as the root user, as described in the [Becoming the Root User \(Server Only\)](#), page 4-2, then enter the following commands:

```
# cd /opt/CSCOsgrm/bin
# ./mwrm cleanall
```

Data removed includes all MWTM data, notes, preferences, security settings, route files (ITP only), GTT files (ITP only), address table files (ITP only), seed files, event filters, report control files, views, message log files, backup files, and report files, as well as any user-created files stored in the MWTM directories.



CHAPTER 3

Setting Up Your Server

This chapter contains:

- [Importing SNMP Community Names from CiscoWorks \(Solaris Only\), page 3-2](#)
- [Changing MWTM Server Poller Settings, page 3-2](#)
- [Changing the Message Display, page 3-4](#)
- [Setting the ITP Point Code Format, page 3-5](#)
- [Connecting a Single-Instance ITP to a Multiple-Instance ITP, page 3-6](#)
- [Enabling SNMP Traps, page 3-7](#)
- [Limiting Traps by IP Address, page 3-9](#)
- [Configuring a Backup MWTM Server, page 3-10](#)
- [Configuring an MWTM Client Connection Timer, page 3-11](#)
- [Enabling the Terminal Server Proxy Service, page 3-11](#)
- [Setting Up TFTP on Your Server \(ITP Only\), page 3-12](#)
- [Configuring Nodes, page 3-14](#)
- [Creating New Troubleshooting Categories and Commands, page 3-23](#)

Importing SNMP Community Names from CiscoWorks (Solaris Only)

You can use the Cisco Mobile Wireless Transport Manager (MWTM) to store all SNMP community names in a single database in CiscoWorks Common Services (CS), and to export those names for use by the MWTM.

To export the database from CiscoWorks CS to the MWTM:

-
- Step 1** Log in to CiscoWorks. From the Common Services tab, choose **Device and Credentials > Device Management**.
- Step 2** Click the **Export** button.
- Step 3** In the tree in the left pane, select the device(s) for export. To choose all devices, click the box next to CS@<your_server_name>. To choose an individual device:
- Expand the hierarchy
 - Drill-down to find an individual device
 - Click the box next to the corresponding device
- Step 4** In the fields in the right pane, enter:
- File Name = mwtm**
Format = CSV
-

CiscoWorks creates the *mwtm* file in the default export directory, */opt/CSCOpX/objects/dmgt*. When you start the MWTM server, the MWTM looks for this file. If the file exists, the MWTM merges the file with its own community name database, and the exported SNMP community names will appear in the SNMP tab of the Node SNMP and Credentials dialog box (see [Configuring Nodes, page 3-14.](#))



Tip

For more information about SNMP, refer to “Configuring SNMP Support” in the Cisco IOS Release 12.2 *Configuration Fundamentals Configuration Guide*, Part 3, System Management.

Changing MWTM Server Poller Settings



Note

For details on changing poller settings using the MWTM client or MWTM web interface, see [Changing Client and Web Preference Settings, page 5-1](#)

The MWTM provides four pollers for use in the MWTM client GUI and web pages: a fast poller, a slow poller, a status refresh poller, and a memory poller. Using the MWTM, you can change the settings (such as minimum, maximum, and default) for each poller. However, the only setting you can modify for the memory poller is the timeout value.

To change server poller settings:

Step 1 Edit the *Server.properties* file:

- If you installed the MWTM in the default directory, */opt*, then the location of the *Server.properties* file is */opt/CSCOsgm/properties/Server.properties*.
- If you installed the MWTM in a different directory, then the *Server.properties* file is located in that directory.

Step 2 To change fast poller settings, change one or more of these lines in the file:

```
# Fast poller default polling interval in seconds
FAST_POLLER_DEFAULT = 15

# Fast poller minimum polling interval in seconds
FAST_POLLER_MIN = 5

# Fast poller maximum polling interval in seconds
FAST_POLLER_MAX = 60
```

For example, to change the fast poller default to 30 seconds, change the `FAST_POLLER_DEFAULT` line to:

```
FAST_POLLER_DEFAULT = 30
```

Step 3 To change slow poller settings, change one or more of these lines in the file:

```
# Slow poller default polling interval in seconds
SLOW_POLLER_DEFAULT = 60

# Slow poller minimum polling interval in seconds
SLOW_POLLER_MIN = 60

# Slow poller maximum polling interval in seconds
SLOW_POLLER_MAX = 300
```

For example, to change the slow poller default to 180 seconds, change the `SLOW_POLLER_DEFAULT` line to:

```
SLOW_POLLER_DEFAULT = 180
```

Step 4 To change status refresh poller settings, change one or more of these lines in the file:

```
# Status refresh default interval in seconds
STATE_REFRESH_DEFAULT = 180

# Status refresh minimum interval in seconds
STATE_REFRESH_MIN = 180

# Status refresh maximum interval in seconds
STATE_REFRESH_MAX = 900
```

For example, to change the status refresh poller default to 300 seconds, change the `STATE_REFRESH_DEFAULT` line to:

```
STATE_REFRESH_DEFAULT = 300
```

Step 5 To change memory poller settings, update the following value:

```
MEMORY_POLLER_TIMEOUT_INCREMENT = 5000
```

Step 6 Save your changes and restart the MWTM server.

Any changes you make take effect when you restart the MWTM server, and are reflected throughout the MWTM client GUI and web pages at that time.

For each of these pollers, remember that, if you set the:

- Minimum interval for a poller to less than 0 seconds, the MWTM overrides that setting and resets the minimum interval to 0 seconds.
- Maximum interval for a poller to less than the minimum interval, the MWTM overrides that setting and resets the maximum interval to be equal to the minimum interval.
- Default interval for a poller to less than the minimum interval, the MWTM overrides that setting and resets the default interval to be equal to the minimum interval.
- Default interval for a poller to more than the maximum interval, the MWTM overrides that setting and resets the default interval to be equal to the maximum interval.



Tip

Due to potential timeouts during memory polling, Cisco does not recommend that you set the memory timeout add-on value to anything less than the default of 5000 milliseconds. If the MWTM encounters memory timeouts during normal day-to-day operations, you can increment this value to alleviate the problem.

Changing the Message Display

These sections contain information about changing the way the MWTM displays and stores messages:

- [Changing the Location of MWTM Message Log Files, page 3-4](#)
- [Changing the Size of the MWTM Message Log Files, page 3-4](#)
- [Changing the Time Mode for Dates in Log Files, page 3-5](#)
- [Changing the Age of the MWTM Message Log Files, page 3-5](#)

Changing the Location of MWTM Message Log Files

By default, all MWTM system message log files are located on the MWTM server at */opt/CSCOsgm/logs*. To change the location of the system message log directory, use the **mwtm msglogdir** command. For more information, see [mwtm msglogdir, page B-46](#).

Changing the Size of the MWTM Message Log Files

To change the size of the message log files, use the **mwtm logsize** command. For more information, see [mwtm logsize, page B-39](#).

Changing the Time Mode for Dates in Log Files

To change the time mode for dates in log files, use the `mwtm logtimemode` command. For more information, see [mwtm logtimemode](#), page B-40.

Changing the Age of the MWTM Message Log Files

To change the number of days the MWTM archives system message log files before deleting them from the MWTM server, use the `mwtm msglogage` command. For more information, see [mwtm msglogage](#), page B-45.

Setting the ITP Point Code Format

You can use the MWTM to set a new point code format for an MWTM server. The MWTM server and all associated MWTM clients use the new point code format. Normally, you need to do this only once, after installation.



Note

When setting the ITP Point Code Format, if a discovery has already occurred, some node and signaling point objects will have been named using the old format. These names will not be affected by the new format. To force the objects to be recreated using the new point code format, you must perform an `mwtm cleandb`.

After you perform the `mwtm cleandb`, the network will need to be discovered again to populate the device names based on the new signaling point format.

The point code format configuration is contained in the *PointCodeFormat.xml* file.

To set the new point code format, log in as the root user, as described in [Starting the MWTM Client](#), page 4-2, or as a superuser, as described in [Specifying a Super User \(Server Only\)](#), page 2-20. Then enter:

```
# cd /opt/CSCosgm/bin
# ./mwtm pcformat [edit | list | master | restore]
```

Where:

- `edit`—Opens the *PointCodeFormat.xml* file for editing, using `$EDITOR` environment variable if set, otherwise uses `vi`.
- `list`—Displays the current contents of the *PointCodeFormat.xml* file.
- `master`—Restores the *PointCodeFormat.xml* file to the default settings.
- `restore`—Restores the *PointCodeFormat.xml* file to the last saved copy.

The *PointCodeFormat.xml* file provides these default point code formats:

- `<Variant value="ANSI" format="8.8.8"/>`—Formats point codes using the 24-bit American National Standards Institute (ANSI) standard format, `xxx.yyy.zzz`, where:
 - `xxx` is the 8-bit network identification
 - `yyy` is the 8-bit network cluster
 - `zzz` is the 8-bit network cluster member

- `<Variant value="China" format="8.8.8"/>`—Formats point codes using the 24-bit China standard format, `xxx.yyy.zzz`, where:
 - `xxx` is the 8-bit network identification
 - `yyy` is the 8-bit network cluster
 - `zzz` is the 8-bit network cluster member
- `<Variant value="ITU" format="3.8.3"/>`—Formats point codes using the 14-bit International Telecommunication Union (ITU) standard format, `x.yyy.z`, where:
 - `x` is the 3-bit zone identification
 - `yyy` is the 8-bit region identification
 - `z` is the 3-bit signal-point
- `<Variant value="NTT" format="5.4.7" readBits="rightToLeft"/>`— Formats point codes using the 16-bit Nippon Telegraph and Telephone Corporation (NTT) standard format, `xx.yy.zzz`, where:
 - `xx` is the 5-bit zone identification
 - `yy` is the 4-bit area/network identification
 - `zzz` is the 7-bit identifier
- `<Variant value="TTC" format="5.4.7" readBits="rightToLeft"/>`— Formats point codes using the 16-bit Telecommunication Technology Committee (TTC) standard format, `xx.yy.zzz`, where:
 - `xx` is the 5-bit zone identification
 - `yy` is the 4-bit area/network identification
 - `zzz` is the 7-bit identifier

As shown previously, the standard point code format for each variant is three octets. (For example, 3.8.3 for ITU.) However, you can also specify a four-octet format for any of the variants. (For example, 4.3.4.3 for ITU.) The total number of bits must still equal 24 for ANSI and China, 14 for ITU, and 16 for NTT and TTC.

For information about customizing the point code formats, including setting a new three-octet or four-octet format, see the detailed instructions in the *PointCodeFormat.xml* file.

Any changes that you make take effect when you restart the MWTM server.

The MWTM preserves customized point code formats when you upgrade to a new version or release of the MWTM.

Connecting a Single-Instance ITP to a Multiple-Instance ITP

You can configure the MWTM to recognize a single-instance ITP connecting to multiple instances on a multiple-instance ITP. In effect, the MWTM views the multiple networks as a single all-encompassing network.

To connect single-instance ITPs to multiple-instance ITPs:

-
- Step 1** Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).
- Step 2** Enter:
- ```
cd /opt/CSCOsgm/bin
./mwtm pcformat edit
```

The `mwtm pcf format edit` command opens the *PointCodeFormat.xml* file for editing. For more information about using this command, see [Setting the ITP Point Code Format, page 3-5](#).

**Step 3** Add these lines to the *PointCodeFormat.xml* file:

```
<NetworkConfig>
 <Network value="Big-Network">
 <Include value="Network-1"/>
 <Include value="Network-2"/>
 <Include value="Network-3"/>
 </Network>
</NetworkConfig>
```

Where:

- *Network-1*, *Network-2*, and *Network-3* are the names of your subnetworks. (This example assumes that you are combining three subnetworks into one.)
- *Big-Network* is the name of the combined network that includes *Network-1*, *Network-2*, and *Network-3*.

In the MWTM, the signaling point Instance Name field displays the subnetwork name (for example, *Network-1*), and the Point Code field displays the name of the combined network (for example, *Big-Network*).

During Discovery, the MWTM assigns a default name to each discovered signaling point. The assigned default name consists of the point code and the combined network name (for example, 3.8.3:Big-Network).

**Step 4** Save your changes to the *PointCodeFormat.xml* file.

**Step 5** Restart the MWTM server. Any changes you made to the *PointCodeFormat.xml* file take effect when you restart the MWTM server.

---

The MWTM preserves the customized network configuration when you upgrade to a new version or release of the MWTM.

## Enabling SNMP Traps

By default, the MWTM cannot receive SNMP traps. To use SNMP traps with the MWTM, you must first configure the MWTM to receive traps.

### Related Topics:

[Integrating the MWTM with Other Products, page 5-39](#)

To view the current trap reception configuration for the MWTM:

---

**Step 1** Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).

**Step 2** Enter:

```
cd /opt/CSCOsrgm/bin
./mwtm trapstatus
```

The MWTM displays the current trap reception configuration for the MWTM, including:

- Whether receiving traps is enabled or disabled
- Which UDP port the MWTM trap receiver is listening on

---

To configure the MWTM to receive traps:

- 
- Step 1** Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).
- Step 2** Enter:
- ```
# cd /opt/CSCOsgrm/bin
# ./mwtm trapsetup
```
- The MWTM displays:
- The MWTM server must also be stopped to perform this operation.
Do you wish to continue? [n]
- Step 3** Type **y** and press **Enter**. The MWTM stops the MWTM Process Manager and all managed processes and displays:
- Would you like to configure MWTM to receive SNMP traps? [yes]
- Step 4** Press **Enter**. The MWTM displays:
- MWTM can receive traps natively on the standard UDP port number 162 or on any other UDP port chosen. If another application is already bound to the SNMP standard trap reception port of 162, an alternate port number for MWTM to receive traps must be specified.
- UDP port number 44750 is the default alternate port.
- Enter trap port number? [162]
- Step 5** By default, nodes send traps to port 162. To accept the default value, press **Enter**.
- Step 6** If your nodes have been configured to send traps to a different port, type that port number and press **Enter**.
- Step 7** By default, the MWTM listens for traps from trap-multiplexing nodes and NMS applications on port 44750. If you want the MWTM to monitor that port, and port 162 is not available on the MWTM server host, type **44750** and press **Enter**.
- Step 8** If trap multiplexing nodes and NMS applications in your network have been configured to send traps to a different port, type that port number and press **Enter**.
- Step 9** If you are a superuser, you must specify a port number that is greater than 1024, then press **Enter**.
- Do not enter a non numeric port number. If you do, you are prompted to enter a numeric port number.
- When you select an SNMP trap port number for the MWTM server, ensure your nodes use the same SNMP trap port number. See the description of the snmp-server host command in the “Preparing to Install the MWTM” chapter of the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for more information.
- Step 10** To accept the default value, press **Enter**; or, type a different location and press **Enter**.
- The MWTM confirms your choices and restarts the MWTM Process Manager and all managed processes.
-

You can change all aspects of MWTM event processing, including the size of the MWTM event database, the maximum length of time the MWTM is to retain events, and the default severity and color associated with each type of event. If a new trap becomes available that is of interest to the MWTM, you can add it to the MWTM event database, enabling the MWTM to recognize and process the new trap. For more information about changing MWTM event processing, see [Changing the Way the MWTM Processes Events, page 9-35](#).

Limiting Traps by IP Address

By default, when you first install the MWTM, all IP addresses are allowed to send traps to the MWTM server. However, you can use the MWTM to limit the IP addresses that can send traps to the server by creating and maintaining the *trapaccess.conf* file.

You can create the *trapaccess.conf* file and populate it with a list of IP addresses that can send traps to the MWTM server. The MWTM receives traps from only those IP addresses, plus the local host. If the file exists but is empty, the MWTM receives traps only from the local host. (The MWTM always receives traps from the local host.)

When you first install the MWTM, the *trapaccess.conf* file does not exist and the MWTM allows all IP addresses to send traps to the MWTM server.

To create the *trapaccess.conf* file and work with the list of allowed IP addresses:

Step 1 Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).

Step 2 Enter:

```
# cd /opt/CSCOs/gm/bin
```

Step 3 Create the *trapaccess.conf* file:

- To create the *trapaccess.conf* file and add a client IP address to the list, enter:

```
# ./mwtm trapaccess add
```

```
Enter address to add: 1.2.3.4
IP Address 1.2.3.4 added.
MWTM server must be restarted for changes to take effect.
Use the following command to restart the server:
mwtm restart
```

- To create the *trapaccess.conf* file and open the file to edit it directly, enter:

```
# ./mwtm trapaccess edit
```

The default directory for the file is located in the MWTM installation directory. If you installed the MWTM:

- In the default directory, */opt*, then the default directory is */opt/CSCOs/gm/etc*.
- In a different directory, then the default directory resides in that directory.

In the *trapaccess.conf* file, begin all comment lines with a pound sign (#).

All other lines in the file are MWTM client IP addresses, with one address per line.

Wildcards (*) are allowed, as are ranges (for example, 1-100). For example, the address *.*.*.* allows all clients to send traps to the MWTM server.

After you create the *trapaccess.conf* file, you can use the full set of mwtm trapaccess keywords to work with the file. For more details, see [mwtm trapaccess](#), page B-75.

Any changes that you make to the *trapaccess.conf* file take effect when you restart the MWTM server.

Configuring a Backup MWTM Server

You can use the MWTM to configure a second MWTM server as a backup for the primary MWTM server. For best results, Cisco recommends that you configure the primary server and the backup server as backups for each other.

To configure a backup MWTM server:

Step 1 Log in as the root user, as described in [Starting the MWTM Client](#), page 4-2, or as a superuser, as described in [Specifying a Super User \(Server Only\)](#), page 2-20.

Step 2 Enter:

```
# cd /opt/CSCOsgrm/bin
# ./mwtm secondaryserver hostname naming-port webport
```

where:

- *hostname* is the optional name of the host on which the backup MWTM server is installed.
- *naming-port* is the optional MWTM Naming Server port number for the backup MWTM server. The default port number is 44742.
- *webport* is the optional MWTM web port number for the backup MWTM server. The default port number is 1774.



Note If you use the mwtm secondaryserver command to configure a backup MWTM server, but the primary MWTM server fails before you launch the MWTM client, then the MWTM client has no knowledge of the backup server.

Step 3 (Optional) To list the backup MWTM server that has been configured for this primary MWTM server, enter:

```
# cd /opt/CSCOsgrm/bin
# ./mwtm secondaryserver list
```

Step 4 (Optional) To configure whether or not a prompt appears on the client in the event of server failover, see [mwtm clientfailoverprompt](#), page B-17.

Configuring an MWTM Client Connection Timer

You can use the MWTM to specify how long an MWTM client is to wait for the MWTM server before exiting.

To configure an MWTM client connection timer:

Step 1 Login as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).

Step 2 Enter:

```
# cd /opt/CSCOsgm/bin
# ./mwtm cliconntimer number-of-seconds
```

where *number-of-seconds* is the time the MWTM client is to wait for a message from the MWTM server before exiting. The valid range is 10 seconds to an unlimited number of seconds. The default value is 60 seconds.

If the timer expires, the client attempts to contact the server and takes one of these actions. If the server:

- Responds to the client, the client reconnects to the server.
- Does not respond to the client, but a backup server is configured, the client attempts to connect to the backup server.
- Does not respond to the client, and no backup server is configured, the client displays a dialog box with this message:

```
Connection to the server has timed out.
Client could not establish 2-way communications with the server.
If you are running through a VPN you may have entered the wrong client IP address.
```

Click **OK** to exit the client. The MWTM writes this message to the client console log:

- Solaris or Linux client—*/opt/CSCOsgmClient/logs/sgmConsoleLog.txt*
- Windows client—*C:\Program Files\Cisco Systems\MWTM Client\logs\consoleLog.txt*

The timer takes effect when you restart the MWTM server.

Step 3 (Optional) To restore the default timeout of 60 seconds, enter:

```
# ./mwtm cliconntimer clear
```

The timer is reset to 60 seconds when you restart the MWTM server.

Enabling the Terminal Server Proxy Service

The MWTM provides the capability to function through firewalls, where the server is located behind the firewall and the client is outside the firewall. To use this feature, enable the terminal proxy service by the `mwtm termproxy` command (see [mwtm termproxy, page B-75](#)).

Setting Up TFTP on Your Server (ITP Only)

Before deploying or loading route table, GTT, or MLR address table files, the TFTP daemon must be running on the Solaris or Linux server.



Tip

For more information about questions regarding TFTP, see [When I try to deploy routes, GTT files, or address table files from the MWTM, why does TFTP fail or time out?](#), page C-14.

This section contains:

- [Setting Up TFTP on Solaris, page 3-12](#)
- [Setting Up TFTP on Linux, page 3-13](#)

Setting Up TFTP on Solaris

To set up TFTP on your Solaris server:

Step 1 Verify that the `tftp-server` package is installed:

```
pkginfo -l | grep tftp
```

If the `tftp-server` package is not installed, install it from your Solaris CD or distribution.

Step 2 If you are not logged in, log in as the root user:

```
> login: root
> Password: root-password
```

If you are already logged in, but not as the root user, use the `su` command to change your login to root:

```
# su
# Password: root-password
```



Caution

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are a relatively inexperienced UNIX user, limit your activities as the root user to the tasks described in this manual.

Step 3 Using a UNIX editor, open the `inetd.conf` file:

```
/etc/inetd.conf
```

Step 4 In the `inetd.conf` file, ensure that this line appears:

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd -s /tftpboot
```

If the line begins with a `#` sign, delete it, and save the changes.

Step 5 Ensure that this directory exists:

```
/tftpboot
```

If not, then create this directory. Also ensure the directory has write permissions (777).

- Step 6** If you will be accessing more than one type of file (route, GTT, or MLR address table files,) you must create subdirectories, for example:

```
/tftpboot/route
/tftpboot/gtt
/tftpboot/atbl
```

- Step 7** Restart the inetd process:

- a. As the root user, enter:

```
# ps -ef | grep inetd
```

Output should be similar to:

```
root    157      1  0   Oct 21 ?           0:00 /usr/sbin/inetd -s
```

- b. To find the process ID for inetd, enter:

```
# ps -e -o pid,comm | grep inetd
```

Output should be similar to:

```
157 /usr/sbin/inetd
```

- c. To restart the inetd process, enter:

```
# kill -HUP 157
```

Where 157 corresponds to the output integer returned in Step b.

- Step 8** Within the */opt/CSCOs/gm/bin* directory, set the staging directory with these commands. For:

- Route table files, use the **mwtm routedir** command (see [mwtm routedir](#), page B-114).
- GTT files, use the **mwtm gttdir** command (see [mwtm gttdir](#), page B-98).
- MLR address table files, use the **mwtm atbldir** command (see [mwtm atbldir](#), page B-90).

Setting Up TFTP on Linux

To set up TFTP on your Linux server:

- Step 1** Verify that the tftp-server package is installed:

```
rpm -q tftp-server
```

If the tftp-server package is not installed, install it from your RedHat Enterprise CD or distribution.

- Step 2** If you are not logged in, log in as the root user:

```
> login: root
> Password: root-password
```

If you are already logged in, but not as the root user, use the “su” command to change your login to root:

```
# su
# Password: root-password
```

**Caution**

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are a relatively inexperienced UNIX user, limit your activities as the root user to the tasks described in this manual.

Step 3 Using a UNIX editor, open the *tftp* file:

```
/etc/xinetd.d/tftp
```

Step 4 Edit the file:

a. Change the line:

```
user = nobody
```

to

```
user = root
```

b. Change the line:

```
disable = yes
```

to

```
disable = no
```

c. If you want to specify a different TFTP directory, replace */tftpboot* in the line *server_args = -s /tftpboot* with the name of your directory.

Step 5 Save the changes.

Step 6 Enter:

```
/etc/init.d/xinetd restart
```

Step 7 Set the staging directory:

- For route table files, use the *mwmt routedir* command (see [mwmt routedir](#), page B-114).
- For GTT files, use the *mwmt gttdir* command (see [mwmt gttdir](#), page B-98).
- For MLR address table files, use the *mwmt atbldir* command (see [mwmt atbldir](#), page B-90).

Configuring Nodes

If MWTM User-Based Access is disabled, or if it is enabled and you are a Network Administrator or System Administrator, you can use the MWTM to view and change SNMP settings and configure login credentials.

For more information about user authorization levels in the MWTM, see [Configuring MWTM User Account Levels \(Server Only\)](#), page 2-7.

To access SNMP and credentials configuration, choose **Network > Node SNMP and Credentials Editor** from the MWTM main menu. The MWTM displays the Node SNMP and Credentials Editor dialog box.

The Node SNMP and Credentials Editor dialog box contains:

- [Node SNMP and Credentials Menu](#), page 3-15

- [Configuring SNMP Settings, page 3-15](#)
- [Configuring Login Credentials, page 3-20](#)

Node SNMP and Credentials Menu

The menu on the Node SNMP and Credentials Editor dialog box contains:

Menu Command	Description
File > Save (Ctrl-S)	Saves any SNMP configuration changes. When you are satisfied with all of your changes to the SNMP settings, choose the File > Save menu option. The MWTM saves the changes and updates the SNMP information on the MWTM server in real time. Note If another user modifies and saves the SNMP configuration before you save your changes, the MWTM asks if you want to overwrite that user's changes. If you choose to do so, the other user's changes are overwritten and lost. If you choose not to do so, your changes are lost.
File > Close (Ctrl-W)	Closes the current window. You may be prompted to save the current changes.
Help > Topics (F1)	Displays the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Displays online help for the current window.
Help > About (F3)	Displays build date, version, SSL support, and copyright information about the MWTM application.

Configuring SNMP Settings



Note

If you want to change SNMP settings, do so *before* running discovery.

For more information about SNMP, refer to “Configuring SNMP Support” in the Cisco IOS Release 12.2 *Configuration Fundamentals Configuration Guide*, Part 3, System Management.

To change SNMP settings in the MWTM, start the MWTM client, as described in [Starting the MWTM Client, page 4-2](#), then choose:

- From the MWTM main window—**Network > Node SNMP and Credentials Editor** from the MWTM main menu.
- From the Discovery Dialog—**Edit > Node SNMP and Credentials Editor** from the menu bar.



Note

(If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator [level 4] and higher.)

The MWTM displays the SNMP tab.

The SNMP tab of the Node SNMP and Credentials Editor dialog box contains:

- [SNMP Settings Table, page 3-16](#)
- [SNMP Configuration Table, page 3-16](#)
- [SNMP Configuration Buttons, page 3-18](#)

The MWTM also provides a set of commands that you can use to configure SNMP settings (see [SNMP Configuration Commands, page 3-18](#)).

SNMP Settings Table

The SNMP settings table displays current SNMP information for nodes in the MWTM. You can edit these fields in the [SNMP Configuration Table, page 3-16](#).

The SNMP configuration table contains:

Column	Description
IP Address Range or Hostname	IP address or DNS name of a node or range of nodes. An asterisk (*) indicates a wildcard value.
Read Community	SNMP community name used by the node for read access to the information maintained by the SNMP agent on the node.
Timeout (secs)	Time, in seconds, the MWTM waits for a response from the node.
Retries	Number of times the MWTM attempts to connect to the node.
Poll Interval (mins)	Time, in minutes, between polls for the node.

SNMP Configuration Table

In the SNMP configuration table, you can change SNMP settings for a node.

The SNMP configuration table contains:

Field	Description
IP Address Range or Hostname	IP address or DNS name of a node. To change the IP address or DNS name of a node, select the node, enter the new address or name in the IP Address Range or Hostname field, then click Update. IP addresses use the format <i>x.x.x.x</i>, where each <i>x</i> has one of these values: • An integer in the range 0 through 255. • A range of integers separated by a hyphen (-), such as 10-60. • An asterisk (*), which is equivalent to specifying 0-255. The default value for this field is the IP address <i>*.*.*.*</i>, which the MWTM uses for all nodes not covered by other IP address ranges or names. When entering an IP address: • Use Class A, B, or C addressing: – Class A—The first octet value is within the range of 1-126. A valid IP address is from 1.0.0.1 to 126.255.255.254. – Class B—The first octet value is within the range of 128-191. A valid IP address is from 128.1.0.1 to 191.254.255.254. – Class C—The first octet value is within the range of 192-223. A valid IP address is from 192.0.1.1 to 223.255.254.254. • Do not use 0 or 255 for the last octet (<i>x.x.x.0</i> is reserved for subnet addresses or network addresses; <i>x.x.x.255</i> is reserved for subnet broadcast addresses). • Do not use IP addresses that fall within these ranges: 127.0.0.1-127.255.255.254, 128.0.0.1-128.0.255.254, 191.255.0.1-191.255.255.254, 223.255.255.1-223.255.255.254, and so on. • Do not use 0 for the first octet. Unlike IP addresses, you cannot specify a range of node names or use wildcards in node names. Each node name corresponds to a single node in the network.
Read Community	SNMP community name to be used by the node for read access to the information maintained by the SNMP agent on the node. To change the SNMP community name for a node, select the node and enter the new name in the Read Community field, then click Update. This new SNMP community name must match the name used by the node. The default name is <i>public</i>. For information about exporting SNMP community names from CiscoWorks Resource Manager Essentials (RME), see Importing SNMP Community Names from CiscoWorks (Solaris Only), page 3-2.

Field	Description
Timeout (secs)	Time, in seconds, the MWTM waits for a response from the node. If you determine that the MWTM waits too long for a response from a node, or does not wait long enough, you can change the timeout value. To change the time that the MWTM waits for a response from a node, select the node and enter the new timeout value in the Timeout (secs) field, then click Update. The valid range is 1 to 60 seconds. The default value is 1 second.
Retries	Number of times the MWTM attempts to connect to the node. If you determine that the MWTM retries a node too many times, or not enough times, you can change the number of retries. To change the number of times the MWTM attempts to connect to a node, select the node and enter the new number in the Retries field, then click Update. The valid range is 0 to 99. The default value is 2 retries.
Poll Interval (mins)	Time, in minutes, between polls for the node. If you determine that the MWTM polls a node too often, or not often enough, you can change the poll interval. To change the time, in minutes, between polls for a node, select the node and enter the new interval in the Poll Interval (mins) field, then click Update. The valid range is 5 to 1440. The default value is 15 minutes.

SNMP Configuration Buttons

The SNMP tab of the Node SNMP and Credentials Editor dialog box contains:

Button	Description
Add	Adds the new SNMP settings to the MWTM database. To add a new node or range of nodes, enter the SNMP information in the appropriate fields and click Add. The new SNMP settings are added to the MWTM database.
Update	Applies the values in the SNMP configuration fields to the selected node or range of nodes.
Delete	Deletes the selected node or range of nodes. To delete a node, select it and click Delete. The MWTM deletes the node without asking for confirmation.

SNMP Configuration Commands

This section contains:

- [MWTM Commands for SNMP, page 3-19](#)
- [Required SNMP Configuration for RAN-O Nodes, page 3-19](#)

MWTM Commands for SNMP

The MWTM provides these SNMP-related commands:

Command	Description
mwtm addsnmpcomm	Adds an SNMP configuration.
mwtm deletesnmpcomm	Deletes an SNMP configuration.
mwtm modifiesnmpcomm	Modifies an existing SNMP configuration.
mwtm showsnmpcomm	Shows SNMP configuration(s).
mwtm snmpcomm	Sets a new default SNMP read community name.
mwtm snmpconf	Changes the file used for SNMP parameters, such as community names, timeouts, and retries.
mwtm snmpget	Queries a host using an SNMP GET request.
mwtm snmpnext	Queries a host using an SNMP GETNEXT request.
mwtm snmpsetup	Sets up SNMP configuration(s).
mwtm snmpwalk	Queries a host using an SNMP GETNEXT request or an SNMP GETBULK request to “walk” through the MIB.



Tip

For more information on the use of these commands, see [Appendix B, “Command Reference.”](#)

Required SNMP Configuration for RAN-O Nodes

Configure these SNMP statements on the RAN-O nodes that you would like to manage by using the MWTM:

```
ipran-mib snmp-access <inBand | outOfBand>
ipran-mib location <cellSite | aggSite>
logging traps informational

snmp-server enable traps syslog
snmp-server community <SNMP_COMMUNITY_STRING> RO 1
snmp-server trap link ietf snmp-server queue-length 100
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server enable traps ipran snmp-server enable traps cpu threshold
snmp-server host <SNMP_SERVER_HOST_IP_ADDRESS> version 2c v2c
```



Tip

For more information about these commands, refer to the *Cisco MWR 1941-DC-A Mobile Wireless Edge Router Software Configuration Guide*.

Configuring Login Credentials

This section contains:

- [Setting Up Login Credentials, page 3-20](#)
- [Credentials Fields, page 3-21](#)
- [Credentials Buttons, page 3-22](#)
- [Adding Nodes, page 3-23](#)
- [Credentials Commands, page 3-23](#)

You can use the MWTM to set up log in credentials, which you may use for:

Action	Description	Related Content
Troubleshooting	All networks	Viewing Troubleshooting
Discovery	ONS nodes only Note Only ONS nodes require login credentials during discovery; all other node types only require an SNMP community string.	Discovery Overview
Deployment	ITP only	Deploying ITP Files
Provisioning	All networks	Using Provisioning
Launching an SSH terminal to a node	All networks In the MWTM client navigation tree, right-click on an object and choose Node > Connect to .	Viewing the Right-Click Menu for an Object
Establishing a low-level connection to a node	ITP only In the MWTM client, choose Network > Node File Management , then choose File > Connect or In the Route Table Editor, choose File > Deploy or In the Global Title Translator Editor or Address Table Editor, choose File > Load from Node or File > Deploy .	Node File Management Deploying ITP Files Loading a GTT File from a Node Loading an Address Table File from a Node

Setting Up Login Credentials

The MWTM enables a system administrator to configure the login credentials using the Node SNMP and Credentials Editor dialog box. Login credentials are stored in an encrypted file on the server, eliminating the need for users to login before running commands.

To set up login credentials in the MWTM, start the MWTM client, as described in [Starting the MWTM Client, page 4-2](#), then choose **Network > Node SNMP and Credentials Editor** from the MWTM main menu, and select the Credentials tab.

**Note**

If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

For detailed information on the SNMP tab, see [Configuring SNMP Settings, page 3-15](#).

**Tip**

A check mark appears beside nodes or default credentials that are configured.

A system administrator can set up credentials:

- Globally on all nodes of all types—Click **Default** and complete the fields in the right pane.
- All nodes of a specific node type only—Under Default, click the node type and complete the fields in the right pane.

**Note**

Configuring default Cell Site Router (CSR) credentials applies to these CSRs: Cisco MWR and Cisco 3825.

- On a specific node—Under Nodes, click the node name and complete the fields in the right pane. Configuring credentials on a specific node overrides any Default credentials for that particular node.

The Credentials tab of the Node SNMP and Credentials dialog box contains:

- [Credentials Fields, page 3-21](#)
- [Credentials Buttons, page 3-22](#)

The MWTM also provides a set of commands that you can use to configure SNMP settings (for details, see the [Credentials Commands, page 3-23](#)).

Credentials Fields

Under the Credentials tab of the Node SNMP and Credentials dialog box, you can configure these login credentials for node(s):

**Note**

Ensure that each user has sufficient privileges to run all commands.

Field	Description
IP Address or DNS Hostname	See Adding Nodes, page 3-23 .
User name	Enter the login user name, if required.
Password	Enter the login password, if required.
Enable User name	Enter the login enable user name (not required for ONS nodes).

Field	Description
Enable Password	Enter the login enable password (not required for ONS nodes).
Connection Protocol	Choose the protocol to use when connecting to the node, either SSH or Telnet. Note The key size on the node must be configured to a minimum of 768 bits and a maximum of 2048 bits.

**Note**

User name and password requirements vary according to your security configuration. For more information, see the *Cisco IOS Security Configuration Guide, Release 12.2, Part 1* and *Part 5*.

Credentials Buttons

The Credentials tab of the Node SNMP and Credentials dialog box contains:

Button	Description
Apply	Applies specified user names and passwords to the selected node or Default credentials.
Clear	Removes credentials. To clear user names and passwords on a selected object, click Clear to remove the credentials, then click Apply .
Test	You can test the credentials you have configured on the corresponding node or the default credentials against a selected node type (not available for all node types).
Add	(Button only available when you click Nodes) Adds a specified node.

Adding Nodes

In the Credentials tab, you can add a node. If you are working with ONS nodes, you must add the ONS node and set the credentials for the node before running discovery.

-
Step 1	Click Nodes in the navigation tree.
Step 2	Enter the IP address or DNS host name.
Step 3	Add the user name and password credentials.
Step 4	Specify the connection protocol (Telnet or SSH).
Step 5	Click Add .
-

Credentials Commands

The MWTM also provides credentials-related commands:

- To add credentials for a given IP address, or for the Default credentials, use the `mwtm addcreds` command.
- To show credentials for a given IP address, or for the Default credentials, use the `mwtm showcreds` command.
- To delete credentials for a given IP address, or for the Default credentials, use the `mwtm deletcreds` command.



Tip

For more information on the use of these commands, see [Appendix B, “Command Reference.”](#)

Creating New Troubleshooting Categories and Commands

A system administrator can use the MWTM to create user-specific categories and commands:

-
Step 1	On the server machine, if you are not logged in, log in as the root user:

```
> login: root
> Password: root-password
```

If you are already logged in, but not as the root user, use the “su” command to change your login to root:

```
# su
# Password: root-password
```



Caution

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are a relatively inexperienced UNIX user, limit your activities as the root user to the tasks described in this manual.

Step 2	Using a UNIX editor, open the <i>UserCommands.ts</i> file:

```
/opt/CSC0sgm/etc/UserCommands.ts
```

- Step 3** Create new categories and commands, following the instructions in the *UserCommands.ts* file. Sample categories and commands are provided, which may be directly useful in your network.
- Step 4** Save changes. The new categories and commands now appear in the Troubleshooting tabs.
-

Related Topics

- [Viewing Troubleshooting, page 8-43](#)
- [mwtm tshootlog, page B-77](#)



CHAPTER 4

Getting Started

This chapter provides information about starting and stopping the Cisco Mobile Wireless Transport Manager (MWTM), and an overview of how to use the MWTM to manage your network.

This chapter includes:

- [Starting the MWTM Server, page 4-1](#)
- [Starting the MWTM Client, page 4-2](#)
- [Discovering Your Network, page 4-4](#)
- [Displaying the MWTM Main Window, page 4-16](#)
- [Using the MWTM Toolbar, page 4-27](#)
- [Using the MWTM Main Menu, page 4-21](#)
- [Accessing the MWTM Through a Web Browser, page 4-28](#)
- [Loading and Saving MWTM Files, page 4-29](#)
- [Using the Windows Start Menu, page 4-30](#)
- [Using the Windows Start Menu, page 4-30](#)
- [Exiting the MWTM Client, page 4-32](#)

For detailed information about the MWTM-supported platforms, and hardware and software requirements, see the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.



Note

The default directory for installing the MWTM is `/opt`. In commands that call for the default directory, if you installed the MWTM in a different directory, you must specify that directory instead of `/opt`.

Starting the MWTM Server

Before starting an MWTM server, verify that:

- Each node uses a supported IOS image
- The MWTM server has IP connectivity to each node
- SNMP is enabled on each node
- (Optional, but recommended) Traps are enabled on each node
- (Optional, but recommended) A trap host is defined on each node

**Tip**

For a definition of MWTM nodes, see [What Is ITP?](#), page 1-6, [What is IPRAN?](#), page 1-7, and [What Is mSEF?](#), page 1-9.

Because the MWTM application comprises a server component and a client component, you must start both components to run the application.

To start the MWTM server on a Solaris or Linux system:

Step 1

You must be logged in as the root user or as a superuser, or your login must have administrator privileges. To log in as the root user, see the [Becoming the Root User \(Server Only\)](#), page 4-2.

**Note**

For details on setting up administrator privileges, see [Specifying a Super User \(Server Only\)](#), page 2-20).

Step 2

Enter:

```
# cd /opt/CSCosgm/bin
# ./mwtm start
```

**Note**

If the database has an exception during start up, the server will fail to start.

Becoming the Root User (Server Only)

Some MWTM procedures require that you log in as the root user.

**Caution**

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use. If you are a relatively inexperienced UNIX user, limit your activities as the root user to the tasks described in this manual.

If you are not logged in, log in as the root user:

```
> login: root
> Password: root-password
```

If you are already logged in, but not as the root user, use the **su** command to change your login to root:

```
# su
# Password: root-password
```

Starting the MWTM Client

This section contains:

- [Before Starting the MWTM Client](#), page 4-3
- [Starting the MWTM Client on Solaris or Linux](#), page 4-3

- [Access the Node, page 4-4](#)
- [Starting the MWTM Client on Windows, page 4-4](#)

Before Starting the MWTM Client

When you start an MWTM client, the version and release of the client must match that of the MWTM server.

If there is a client-server mismatch, the MWTM displays a warning message when you try to start the client. If you have a web browser installed, the MWTM optionally opens a web page from which you can download an allowed, matching client. For more information about downloading the MWTM client, see [Downloading the MWTM Client from the Web, page 11-9](#).

Setting the DISPLAY Variable for Solaris or Linux Clients

If you see the following message upon client startup, you must set the DISPLAY variable:

```
Could not launch client: Can't connect to X11 window server using <x> as the value of the DISPLAY variable.
```

The DISPLAY variable is set as part of your login environment on Solaris or Linux. However, if you use Telnet or SSH to access a workstation, you must set the DISPLAY variable to local display by using this command:

```
# setenv DISPLAY local_ws:0.0
```

where *local_ws* is your local workstation.

If your shell does not support the **setenv** command, enter:

```
# export DISPLAY=local_ws:0.0
```

Starting the MWTM Client on Solaris or Linux

To start the MWTM client on a Solaris or Linux system on which the MWTM server is installed, ensure that the MWTM server is running, then enter:

```
# cd /opt/CSCosgm/bin
# ./mwtm client
```

To start the MWTM client on a Solaris or Linux system other than the one on which the MWTM server is installed, ensure that the MWTM server is running, then enter:

```
# cd /opt/CSCosgmClient/bin
# ./mwtm client
```

To start the MWTM client on a Solaris or Linux system other than the one on which the MWTM server is installed, and connect to an MWTM server other than the default server, enter:

```
# cd /opt/CSCosgmClient/bin
# ./mwtm client server_name_or_ip_address
```

where *server_name_or_ip_address* is the name or IP address of the Solaris or Linux system on which the MWTM server is running.

Access the Node

You use the MWTM to link to the node by using the connection protocol (Telnet or SSH) that you set in the Node SNMP and Credentials dialog box (see [Credentials Fields, page 3-21](#)).

To access the node, right-click a node in a window, then choose **Node > Connect to** from the right-click menu.

**Note**

If your client workstation does not have network access to the IP address of the node (that is, if the node is behind a firewall or NAT device), you might be unable to access the node.

Starting the MWTM Client on Windows

To start the MWTM client on a Windows system, choose **Start > Programs > Cisco MWTM Client > Launch MWTM Client**, or double-click the MWTM Client icon on the Windows desktop.

Discovering Your Network

This section provides details on using the MWTM to discover your networks. It includes:

- [Discovery Overview, page 4-4](#)
- [Launching the Discovery Dialog, page 4-6](#)
- [Loading Seed Nodes and Seed Files, page 4-7](#)
- [Running Discovery, page 4-12](#)
- [Verifying Discovery, page 4-15](#)

Discovery Overview

The MWTM uses a Discovery process to populate the MWTM database, discovering the objects in your network.

You can run Discovery if MWTM User-Based Access is disabled; or, if it is enabled, and you are a Network Administrator or System Administrator. (For more information about user authorization levels in the MWTM, see [Configuring MWTM User Account Levels \(Server Only\), page 2-7](#).)

To discover your network:

-
Step 1	Start the MWTM client, as described in Starting the MWTM Client, page 4-2 .
Step 2	If you want to change SNMP settings, do so <i>before</i> running Discovery. See Configuring SNMP Settings, page 3-15 for more information.
Step 3	If you want to discover ONS nodes and did not choose the option to discover your network during installation, you must add the ONS nodes and set the credentials before running discovery (see Adding Nodes, page 3-23 for more information.)
Step 4	Choose Network > Network Discovery from the MWTM main menu. The MWTM displays the Discovery dialog box. See Launching the Discovery Dialog, page 4-6 for more information.

- Step 5** Select the **Seed Settings** tab, if it is not already chosen. You use the Seed Settings tab to create, save, load, and delete MWTM seed files. Load one or more seed nodes, or an existing seed file, by using the procedures in [Loading Seed Nodes and Seed Files, page 4-7](#).
- Step 6** Select the **Discovery** tab, or click **Next**. You use the Discovery tab to discover the objects in your network. See [Running Discovery, page 4-12](#) for more information.
- To specify the extent of the network discovery, check the **Entire Network** check box. See the description of the Entire Network check box in [Running Discovery, page 4-12](#) for more information.
 - To specify whether the MWTM should keep or delete the existing database when discovering the network, check the **Delete Existing Data** check box. See the description of the Delete Existing Data check box in [Running Discovery, page 4-12](#) for more information.
 - To specify the maximum number of hops for discovering objects in your network, enter a value in the **Max. Hops** text box. For more information, see the description of the Max. Hops text box in the [Running Discovery, page 4-12](#).
- Step 7** Click the **Discover Network** button.

When the “Discovery In Progress” message disappears, discovery is running. The Discovered Nodes table in the Discovery tab lists all nodes that the MWTM discovered (all nodes, including new and excluded nodes, not just the nodes in the current view). See [Discovered Nodes, page 4-15](#) for more information.



Note Event processing in the MWTM might experience congestion when discovering very large networks. If the number of events exceeds the capacity of the event queue, the event congestion icon  appears in the lower left of the MWTM client and web windows. If the icon appears, the presentation of event information in the MWTM will lag behind the actual state of the network objects until the congestion clears. No user action is necessary.

- Step 8** Examine the Discovered Nodes table to verify that the MWTM discovered all of the nodes in the network. If you suspect that the MWTM did not discover all of the nodes, see [Verifying Discovery, page 4-15](#) for troubleshooting information. You might need to add more seed nodes and run discovery again.
- Step 9** When you are satisfied that the MWTM discovered all of the nodes in the network, save the list of seed nodes in a seed file. See [Saving a Seed File, page 4-8](#) for more information.



Note (ITP only) You can run discovery multiple times to attempt to discover additional nodes based on the IP addresses defined in the Stream Control Transmission Protocol (SCTP) links. If you are using a separate management VLAN to manage your nodes, but private or unreachable IP addresses for your SCTP connectivity, uncheck the **Entire Network** check box in the Discovery dialog box. Otherwise, discovery attempts to reach those nodes continuously. Instead, enter all nodes to be discovered directly into the seed list and do a nonrecursive discovery.

Related Topics:

- [Configuring SNMP Settings, page 3-15](#)
- [Backing Up or Restoring MWTM Files \(Server Only\), page 2-32](#)
- [Investigating Data Problems, page D-1](#)

Launching the Discovery Dialog

To launch the Discovery dialog box and begin the Discovery process, choose **Network > Network Discovery** from the MWTM main menu. The MWTM displays the Discovery dialog box.

You use the Discovery dialog box to load and configure seed nodes, and use those seed nodes to discover the objects in your network.

If you start the MWTM client and the MWTM database is empty (including the very first time you start the MWTM client), the MWTM automatically opens the Discovery dialog box so you can run Discovery and populate the database.

The Discovery dialog box contains:

- [Discovery Dialog Menu, page 4-6](#)
- [Discovery Dialog Tabs, page 4-6](#)

Discovery Dialog Menu

The menu on the Discovery dialog box contains:

Menu Command	Description
File > Load Seeds (Ctrl-L)	Opens the Load File Dialog: Seed File List, enabling you to load a seed file into the MWTM: • Enter the name of the seed file, and click OK to load it. • Click Cancel to return to the Seed Settings tab without loading a seed file.
File > Save Seeds (Ctrl-S)	Opens the Save File Dialog: Seed File List, which you use to save changes you have made to the chosen seed file.
File > Save As	Opens the Save File Dialog: Seed File List, which you use to save changes you have made to the chosen seed file with a new name, or overwrite an existing seed file.
File > Close (Ctrl-W)	Closes the current window.
Edit > Node SNMP and Credentials Editor (Alt-D)	Opens the Node SNMP and Credentials Editor dialog box. If you have implemented MWTM User-Based Access, this option is available to users with authentication-level Network Administrator (level 4) and higher.
Help > Topics (F1)	Displays the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Displays online help for the current window.
Help > About (F3)	Displays build date, version, SSL support, and copyright information about the MWTM application.

Discovery Dialog Tabs

The Discovery dialog box contains these tabs:

Tab	Description
Seed Settings	Displays the Seed Settings tab in the Discovery dialog box.
Discovery	Displays the Discovery tab in the Discovery dialog box.

Loading Seed Nodes and Seed Files

You use the MWTM to load one or more new seed nodes; or, to create, save, load, and delete existing MWTM seed files.

This section includes:

- [Loading a Seed Node, page 4-7](#)
- [Loading a Seed File, page 4-7](#)
- [Saving a Seed File, page 4-8](#)
- [Creating a New Seed File, page 4-10](#)
- [Creating a New Seed File, page 4-10](#)
- [Creating and Changing Seed Files Using a Text Editor, page 4-12](#)

Loading a Seed Node

To load a seed node, enter the name or IP address of the seed node in the IP Address, Address range, Subnet, CIDR, or DNS Hostname field, and click **Add Node** (or press **Enter**).

**Note**

Follow the guidelines for IP addresses in [SNMP Configuration Table, page 3-16](#).

The MWTM displays details of the SNMP settings for the seed nodes in the Seed Details pane. Continue adding seed nodes until you are certain that the MWTM will be able to discover the entire network.

Loading a Seed File

If you have already created and saved one or more seed files, you can load a seed file, change the list of seed files, and select one seed file to be loaded automatically when the MWTM client is started or the Discovery dialog box is opened.

To load an existing seed file, choose **File > Load Seeds** from the Discovery Dialog menu. The MWTM displays the Load File Dialog: Seed File List dialog box.

The Load File Dialog: Seed File List contains:

Field or Button	Description
Type	Icon indicating whether the item in the table is a file or a folder.
Name	Name of the seed file or folder.
Last Modified	Date and time the seed file or folder was last modified.
Size (bytes)	Size of the seed file or folder, in bytes.

Field or Button	Description
Make this my preferred start option	Specifies whether the chosen seed file should be loaded automatically whenever this MWTM client is started or the Discovery dialog box is opened. By default, this check box is unchecked for all seed files. That is, no seed file is loaded automatically when the MWTM client is started or the Discovery dialog box is opened.
Number of Files (appears in bottom-left corner)	Total number of seed files and folders.
OK	Loads the chosen seed file, saves any changes you made to the list of files, and closes the dialog box. To load a seed file, double-click it in the list, select it in the list and click OK , or enter the name of the file and click OK . The MWTM saves any changes you made to the list of files, closes the Load File Dialog: Seed File List dialog box, loads the seed file, and returns to the Discovery dialog box. The MWTM lists all of the seed nodes in the seed file in the Seed Nodes pane, and displays details of the SNMP settings for the seed nodes in the Seed Details pane.
Delete	Deletes the chosen file from the seed file list. The MWTM issues an informational message containing the name and location of the deleted file.
Cancel	Closes the dialog box without loading a seed file or saving any changes to the seed file list.
Help	Displays online help for the dialog box.

Saving a Seed File

You use the MWTM to save a specific seed file, change the list of seed files, and select one seed file to be loaded automatically when the MWTM client is started or the Discovery dialog box is opened.

When you are satisfied that the MWTM has discovered all of the nodes in the network, save the list of seed nodes in a seed file by using one of these procedures:

- To save the changes you made to the seed file without changing the name of the file, choose **File > Save** from the Discovery Dialog menu.
- To save the changes you have made to the seed file with a new name, choose **File > Save As** from the Discovery Dialog menu. The MWTM displays the Save File Dialog: Seed File List dialog box.

The MWTM stores the seed file in the seed file directory on the MWTM server:

- If you installed the MWTM in the default directory, */opt*, then the MWTM seed file directory is */opt/CSCOs/gm/seeds*.
- If you installed the MWTM in a different directory, then the MWTM seed file directory is located in that directory.

**Note**

If another user modifies and saves the seed file before you save your changes, the MWTM asks if you want to overwrite that user's changes. If you choose to do so, the other user's changes are overwritten and lost. If you choose not to do so, your changes are lost, unless you save the seed file to a different filename.

The Save File Dialog: Seed File List contains:

Field or Button	Description
Type	Icon indicating whether the item in the table is a file or a folder.
Name	Name of the seed file or folder.
Last Modified	Date and time the seed file or folder was last modified.
Size (bytes)	Size of the seed file or folder, in bytes.
Filename	Name by which you want to save the seed file. If you create a new seed filename, you can use any letters, numbers, or characters in the name that are allowed by your operating system. However, if you include any spaces in the new name, the MWTM converts those spaces to hyphens. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i> .
Make this my preferred start option	Specifies whether the chosen seed file should be loaded automatically whenever this MWTM client is started or the Discovery dialog box is opened. By default, this check box is unchecked for all seed files. That is, no seed file is loaded automatically when the MWTM client is started or the Discovery dialog box is opened.
Number of Files (visible in bottom left corner)	Total number of seed files and folders.
OK	Saves the seed file and any changes you made to the seed file list and closes the dialog box. To save the seed file with a new name, you can either save the file with: • A completely new name. Enter the new name and click OK. • An existing name, overwriting an old seed file. Select the name in the list and click OK. The MWTM: • Saves the seed file with the new name • Saves any changes you made to the list of files • Closes the Save File Dialog: Seed File List dialog • Returns to the Discovery dialog box
Delete	Deletes the chosen file from the seed file list. The MWTM issues an informational message containing the name and location of the deleted file.

Field or Button	Description
Cancel	Closes the dialog box without saving the seed file or saving any changes to the seed file list.
Help	Displays online help for the dialog box.

Creating a New Seed File

To create a new seed file in the MWTM, launch the Discovery dialog box, as described in [Launching the Discovery Dialog, page 4-6](#), then click the **Seed Settings** tab, if it is not already chosen.

You use the Seed Settings tab in the Discovery dialog box to create, save, load, and delete MWTM seed files.

The Seed Settings tab on the Discovery dialog box contains:

Field or Button	Description
Seed Nodes	Lists the seed nodes currently defined in the MWTM.
IP Address Range or Hostname	IP address of the seed node. The default value is *.*.*.*. Note Follow the guidelines for IP addresses in SNMP Configuration Table, page 3-16 .
Retries	Number of times the MWTM attempts to connect to the seed node. The valid range is 0 to 99. The default value is 2.
Timeout (sec)	Time, in seconds, the MWTM waits for a response from the seed node. The valid range is 0 (no timeout) to 9999. The default value is 1 second.
Read Community	SNMP community name for read access to the information maintained by the SNMP agent on the node. This value can be up to 32 characters in length. Do not include special characters such as the opening single quote ('), at symbol (@), dollar sign (\$), caret (^), closing single quote ('), double quote ("), ampersand (&), or pipe (). This value is usually set to public (the default).
Poll Interval (mins)	Time, in minutes, between polls. The valid range is 0 to 9999. The default value is 15 minutes.

Field or Button	Description
IP Address, Address range, Subnet, CIDR, or DNS Hostname	Address or name of the chosen seed node. To create a new seed file, enter the name or address of a seed node in this field. Examples of acceptable input include: • IP Address: 1.2.3.4 (see the guidelines for IP addresses in SNMP Configuration Table, page 3-16). • Address Range: 1.2.3.2-15 • Subnet, CIDR: 1.2.3.0/24, 1.2.3.0/255.255.255.0 • DNS Hostname: mwtm.cisco.com The MWTM displays details of the SNMP settings for the seed node in the Seed Details pane. Continue to add as many seed nodes as necessary to discover your entire network. When you are ready to save the list of seed nodes in a new seed file, choose File > Save As from the Discovery Dialog menu. The MWTM displays the Save File Dialog: Seed File List dialog box. See Saving a Seed File, page 4-8, for more information about saving seed files.
Add Node	Adds a new seed node to the MWTM.
Delete	Deletes the chosen seed node. The MWTM deletes the seed node without asking for confirmation.
Next	Displays the Discovery tab in the Discovery dialog box. If you enter a seed node IP address or name in the IP Address, Address range, Subnet, CIDR, or DNS Hostname field, then click Next, MWTM automatically adds the seed node before displaying the Discovery tab.

Changing an Existing Seed File

To modify an existing seed file in MWTM:

-
- Step 1** Load the seed file as described in [Loading a Seed File, page 4-7](#).
- Step 2** To add another seed node to the seed file, enter the name or IP address of the seed node in the IP Address, Address range, Subnet, CIDR, or DNS Hostname field, and click **Add Node**.
- Step 3** To delete a seed node from the seed file, select the seed node and click **Delete Node**.
- Step 4** To save the modified seed file, use the procedure described in [Saving a Seed File, page 4-8](#).
-

Creating and Changing Seed Files Using a Text Editor

A seed file is simply an unformatted list of seed node names. To create a seed file by using a text editor, simply create a file and list the seed node names, one on each line, with no other formatting:

```
new-york-a
new-york-b
chicago-c
```

When you save and name the seed file, remember:

- You can use any letters, numbers, or characters in the name that your operating system allows, except blanks.
- The MWTM saves the seed file with a *.see* file extension.
- The MWTM saves the seed file in the MWTM server's seed file directory, *seeds*:
 - If you installed the MWTM in the default directory, */opt*, then the seed file directory is */opt/CSCOsgm/seeds/*.
 - If you installed the MWTM in a different directory, then the seed file directory resides in that directory.

When the MWTM loads the seed file, it verifies the syntax of the file, deleting blank lines and extraneous leading and trailing spaces as needed. The MWTM also verifies that each seed node name resolves to a valid IP address. If a name does not resolve to a valid IP address, the MWTM logs the erroneous entry and ignores it.

For example, given this seed file:

```
new-york-a<space>
<space>new-york-b
zzzzzzzzzzzz
<blank line>
<tab>chicago-c<tab>
```

The MWTM loads these entries:

```
new-york-a
new-york-b
chicago-c
```

Running Discovery

Click the Discovery tab in the Discovery dialog box to discover the objects in your network.

To display the Discovery tab, launch the Discovery dialog box, as described in [Launching the Discovery Dialog, page 4-6](#), then select the **Discovery** tab in the Discovery dialog box, or click **Next** in the Seed Settings tab. (If you enter a seed node IP address or name in the IP Address, Address range, Subnet, CIDR, or DNS Hostname field, then click **Next**, MWTM automatically adds the seed node before displaying the Discovery tab.)

The Discovery tab comprises:

- [Discovery Settings, page 4-13](#)
- [Discovered Nodes, page 4-15](#)

Related Topics:

- [Discovery Overview, page 4-4](#)

- [Polling a Node, page 8-53](#)

Discovery Settings

The Discovery Settings pane of the Discovery tab contains:

Field or Button	Description
Entire Network	Check box used to specify the extent of the network discovery: • To discover the entire network, check this check box. This is called <i>recursive discovery</i>, and it is the default setting. With this check box checked, the MWTM discovers all seed nodes and attempts to manage them; then attempts to discover and manage all nodes that are adjacent to those seed nodes (unless the nodes are connected by serial links only); then attempts to discover and manage all nodes that are adjacent to <i>those</i> nodes; and so on, until the Max Hops limit is reached. • To rediscover only seed nodes, uncheck this check box. This is called <i>nonrecursive discovery</i>. With this check box unchecked, the MWTM discovers all seed nodes and attempts to manage them, then labels all nodes that are adjacent to those seed nodes as Unmanaged.
Delete Existing Data	Check box used to keep or delete the existing MWTM database when discovering the network: • To keep all existing network data in the MWTM database before rediscovering the network, uncheck this check box. This is the default setting. • To delete all existing network data from the MWTM database before rediscovering the network, check this check box. Choose this option if you know that network elements have been deleted from your network since the last Discovery. If you discover the network with Delete Existing Data chosen, the MWTM stops any real-time polls that are running and issues appropriate messages.
Max Hops	The maximum number of hops from the seed node to search for other nodes to discover. Default is 3.

Field or Button	Description
Discover Network	Begins discovering the network. Click Discover Network to begin Discovery. If you have not defined at least one seed node in the Seed Settings tab, the MWTM prompts you to do so. When Discovery begins: • The Discover Network button changes to Stop Discovery. • The <i>Discovery In Progress</i> message appears in the title bar of all MWTM client windows. Discovery progresses in bursts. You might see a number of updates, followed by a pause, followed by more updates. The information that MWTM windows displays is not fully updated until Discovery is complete. By default, Discovery times out after 600 seconds (10 minutes). To change the Discovery timeout, change the value of the <code>DISCOVERY_TIMELIMIT</code> entry in the <i>Server.properties</i> file: • If you installed the MWTM in the default directory, <i>/opt</i>, then the location of the <i>Server.properties</i> file is <i>/opt/CSCOsgm/properties/Server.properties</i>. • If you installed the MWTM in a different directory, then the <i>Server.properties</i> file resides in that directory. Because the MWTM is an asynchronous system, with the MWTM server contacting clients one at a time, and because clients might run at different speeds, the information that MWTM clients display during Discovery might not always be synchronized. All other MWTM windows (Node, topology, and so on) are also populated with the newly discovered network data.
Stop Discovery	Stops the Discovery process. For example, if you click Discover Network, then you realize that you loaded a seed node that you did not intend to load, you can click Stop Discovery to stop the Discovery process. Note If you stop the Discovery process, the information in the MWTM database is incomplete and unreliable. To generate a new, complete, and reliable MWTM database, check the Delete Existing Data check box and run Discovery again. This button replaces the Discover Network button when the Discovery process begins, and changes back to the Discover Network button when the Discovery process ends.

If you run Discovery with the Entire Network check box unchecked, and then you run Discovery with the Entire Network check box checked, any Unmanaged nodes in the first Discovery are not rediscovered by the second Discovery.

To recover from this situation and generate a new, complete, and reliable MWTM database, you must perform one of these procedures:

- Run Discovery again, with **Entire Network** and **Delete Existing Data** checked.
- Change the Unmanaged nodes to managed status. See [Unmanaging and Managing Nodes or ITP Signaling Points, page 6-42](#), for more information.
- Poll the nodes that were Unmanaged in the first Discovery. See [Polling a Node, page 8-53](#), for more information.

Discovered Nodes

The table in the Discovery tab lists all nodes that the MWTM discovered (all nodes, including new and excluded nodes, not just the nodes in the current view). By default, this table is sorted by Status.

- To see a tooltip for each column in the table, place the cursor over a column heading.
- If a cell is too small to show all of its data, place the cursor over the cell to see the full text in a tooltip.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Discovered Nodes section except Internal ID, Uptime, Reboot Reason, Process Traps, and Last Status Change.

- To display hidden columns, right-click in the table heading and select the check boxes for the columns that you want to display.
- To hide columns, right-click in the table heading and uncheck the check boxes for the columns that you want to hide.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

See [Nodes Table, page 6-5](#), for descriptions of the columns and check boxes of the discovered nodes table.

Verifying Discovery

After you discover the network (see [Discovery Overview, page 4-4](#)), examine the Discovered Nodes table to verify that the MWTM discovered all of the nodes in the network. If you suspect that the MWTM did not discover all of the nodes, verify that:

- No nodes are excluded from your current view.
- The MWTM server can ping the nodes.
- The nodes are running images that are compatible with the MWTM server.
- SNMP is enabled on the nodes.
- The MWTM is configured with the correct SNMP community name. See [Launching the Discovery Dialog, page 4-6](#) for details.
- (ITP only) The missing nodes are connected to the seed nodes by SCTP connections, not just serial connections. If they are not connected by SCTP connections, you must add the missing nodes to the seed file as seed nodes. See [Changing an Existing Seed File, page 4-11](#) for more information.
- You chose Entire Network when you ran Discovery. If you suspect that you did not, run Discovery again with Entire Network chosen.

Displaying the MWTM Main Window

The MWTM main window ([Figure 4-1](#)) is the primary MWTM web client window. It is the first window to appear when you launch the MWTM client.

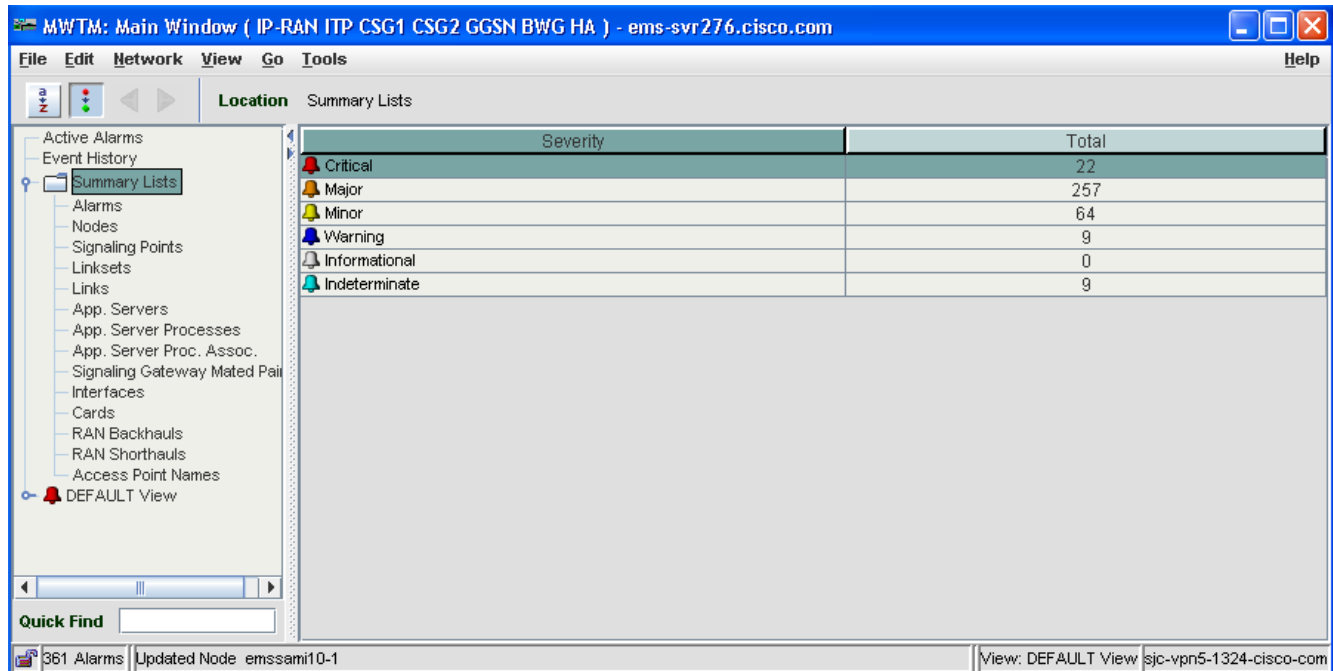
The MWTM main window displays information about the events and objects that the MWTM discovers. The MWTM main window is divided into two primary areas: the navigation tree in the left pane and the content area in the right pane. When you select an item in the navigation tree, MWTM displays detailed information about the item in the content area in the right pane, such as configuration details and real-time data.

The MWTM main window contains:

Element	Description
Title bar	MWTM main window title bar that displays: MWTM main window <(networks)> - <server name>.
Main menu	Main menu on the MWTM main window. For details, see Using the MWTM Main Menu, page 4-21 .
Toolbar	Toolbar options on the MWTM main window. For details, see Using the MWTM Toolbar, page 4-27 .
Navigation tree	Contains lists of objects and views. For details, see MWTM Client Navigation Tree, page 4-19 .
Content area	Contains content for the object chosen in the navigation tree. For details, see MWTM Client Content Area, page 4-19 .

When you start the MWTM for the first time, the MWTM displays the Discovery dialog box and the MWTM main window. See [Figure 4-1](#).

Figure 4-1 MWTM Web Interface



If you have already run Discovery, the events and objects that the MWTM discovered appear in the navigation tree and content area.

When you start the MWTM for the first time, if you did not configure the MWTM server to automatically discover your network the first time the server starts after installation, the Discovery dialog comes up automatically. Until you perform a discovery, the MWTM database contains no information, and the navigation tree and content area are blank. For details on the Discovery dialog, see [Discovering Your Network](#), page 4-4.

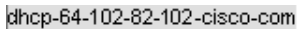
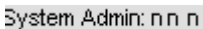
Navigational Features

To help you keep track of which view you are currently using, as well as other important information, most MWTM windows display the name of the system on which the MWTM server is running in the title bar.

On the MWTM toolbar, there is a Location object that shows where you are currently in the MWTM navigation. For more information, see [Using the MWTM Toolbar](#), page 4-27.

At the bottom of the MWTM main window, the following information may appear:

Information	Description
 Locked padlock icon	Appears if the MWTM server has a security certificate. To see the certificate, click the symbol.
 Unlocked padlock icon	Appears if the MWTM server does not have a security certificate.

Information	Description
 Number of objects	(Applicable for Active Alarms, Event History, and all Summary Lists) Shows the number of objects currently visible in the window, if any.
 Number of files	(Only for load or save dialog boxes) Shows the number of files currently visible in the load or save files dialog box, if any.
 Status messages	- Informational messages are visible in black. For example: <code>Discovery running</code> - Messages that indicate successful actions are visible in green. For example: <code>View Saved</code> - Error messages are visible in red. For example: <code>Node does not have a note</code> - The MWTM contains many fields into which you can enter information, such as a new node name or IP address. If you enter an incorrect value in the field, such as an IP address that contains letters or is too long, the MWTM alerts you of the incorrect value and retains the current value of the field. Check the message bar at the bottom of the window for information and assistance.
 Changed	Appears if you have changed but not yet saved a view. You must save the view if you want to save your changes. For details, see Saving a View, page 7-6 .
 New icon	Appears if there is at least one newly discovered object in the network that has not been added to your current view. To add or exclude the object to your current view, see New on the Network Pane, page 7-12. Note Clicking the New icon in the topology window opens the New Objects pane in the left pane. Clicking the New icon in any other window opens the Edit View tab of the View Editor window.
 View	Shows the name of the current view. Note If your personal default view has been deleted, then the next time you launch the client, the MWTM informs you that your default view has been deleted and that your view has been reset to the DEFAULT view. To choose another view as your default view, use the Load Dialog: View List. For details, see Loading a Client-Specific View, page 7-15.
 Name	Shows the name of the current user, or the name of the node the user is using.
 Authentication level	If you have implemented MWTM user access security, the authentication level of the user appears.

MWTM Client Navigation Tree

The MWTM client navigation tree displays objects in a variety of formats and views. The DEFAULT view, and other views that you can create, display a hierarchy of the objects that the MWTM manages. By default, the navigation tree is sorted by alarm severity, with objects having the most severe alarms appearing at the top of the tree.

**Note**

To learn more about alarm severity, see [Chapter 9, “Managing Alarms and Events.”](#)

The client navigation tree contains:

Object	Description
Active Alarms	Displays a summary of all currently active alarms in your network, including the current status of the associated network object. For details, see Chapter 9, “Managing Alarms and Events.”
Event History	Displays information about the events that the MWTM event logger and event processor deliver for all objects in the current network view. For details, see Chapter 9, “Managing Alarms and Events.”
Summary Lists	Displays basic summary alarm information about all discovered network objects, including alarm severity and the total number of objects in each severity level. For details, see Displaying Summary Lists Alarms, page 4-19 .
DEFAULT View (or named view)	Displays the view name and all objects in that view. For details about views, see Chapter 7, “Managing Views.”

**Note**

For additional features that appear only in the navigation tree of the web interface, see [MWTM Web Interface Navigation Tree, page 11-3](#).

MWTM Client Content Area

The content area in the right pane displays detailed information about your network, such as configuration and historical data. To view detailed information for an object, click the object in the navigation tree. The content area in the right pane shows the details about the chosen object.

The content area formats the information in a way that is easy to interpret. Descriptive information is usually organized into subpanes. Tabs along the top of the content area organize more complex sets of information. Large amounts of information are organized into tables with labeled columns and multiple rows of data.

For additional features that appear only in the content area of the MWTM web interface, see [MWTM Web Interface Content Area, page 11-4](#).

Displaying Summary Lists Alarms

Summary Lists provides basic summary alarm information about all discovered network objects, including alarm severity and the total number of objects for each severity level.

**Note**

If you click to expand the turner  beside Summary Lists, all discovered object types in your network appear. For detailed information, see [Displaying Object Windows, page 6-2](#).

To view the summary lists, click Summary Lists in the navigation tree in the MWTM main window. The Summary Lists table has two columns: Severity and Total. You can resize each column, or sort the table based on the information in one of the columns. By default, this table is sorted by Severity, with the highest severity (Critical) at the top. The Total column lists the total number of discovered objects for each severity level.

**Note**

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The summary list table contains:

Column	Description
Severity	Alarm severity of the object. Possible values are:  Critical (red bell)  Major (orange bell)  Minor (yellow bell)  Warning (blue bell)  Informational (gray bell)  Indeterminate (cyan bell)
Total	Total number of network objects with the indicated severity.

**Note**

See [Chapter 9, “Managing Alarms and Events”](#) for information on alarm management.

Right-Click Menu for the Summary Lists

To see the right-click menu for the summary lists, select Summary Lists or any of the objects under Summary Lists in the navigation tree and press the right mouse button. The menu provides:

Menu Command	Description
Show In New Window	Opens the current window in a new window.
Back > List of Windows	Navigates back to a window viewed in this session. The MWTM maintains a list of up to 10 Back windows.
Forward > List of Windows	Navigates forward to a window viewed in this session. The MWTM maintains a list of up to 10 Forward windows.

Using the MWTM Main Menu

The MWTM main menu appears in the menu bar of most MWTM windows.

Some menu items do not appear on some windows. In addition, menu items that are dimmed are not available on that window.

For detailed information about the menu options provided by other windows, see the descriptions of those windows.

The MWTM main menu contains:

Menu Command	Description
File > Load DEFAULT View (Ctrl-D)	Loads the DEFAULT view, which is the view into which the MWTM places all discovered objects when discovering the network. The DEFAULT view is stored on the MWTM server and shared by all MWTM clients, but the clients cannot modify it.
File > Load View (Ctrl-L)	Loads an already existing view. The MWTM prompts you for the name of the view you want to load: - Select the name of the view, or accept the default view name, then click OK to load the view. - Click Cancel to close the prompt window without loading a view.
File > Save View (Ctrl-S)	Saves the current view: - If you have not already saved the current view, opens the Save File dialog box: View List, in which you enter or select a filename under which to save the current view. - If you have already saved the current view, saves the view to that filename. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
File > Save View As	Opens the Save File Dialog: View List, which you use to enter or select a filename under which to save the current view. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
File > Connect to New Server (Ctrl-O)	Connects to a new server. The MWTM prompts you for the new server's name or IP address, and UDP port number. The MWTM stops the MWTM client, then restarts the client connected to the new server.

Menu Command	Description
File > Print (Ctrl-P)	Opens the Print window where you can: • Specify options for printing • Print the current window • Save the current window to a file The MWTM printing options require that you define a printer on your system. If you choose File > Print and the Print window does not appear, ensure you have defined a printer on your system.
File > Exit (Ctrl-Q)	Exits the MWTM application, after prompting you for confirmation. If you are working in a custom view (that is, not the DEFAULT view), the MWTM automatically saves any changes you made to the view.
Edit > Views (Ctrl-M)	Opens the View Editor window to allow you to edit any views that you have created.
Edit > Clear All Events (Ctrl-E)	Deletes the event icon (orange triangle) from MWTM displays for all known objects. The actual events are not deleted from the MWTM, only the event icon for all known objects. Note During Discovery, the MWTM might flag most objects with an event icon. If the event icons are too distracting, use the Edit > Clear All Events menu option to remove them.
Edit > Find (Ctrl-F)	Opens the Find dialog box, in which you find a specific object, event, or text in the window. If you select an object in the navigation tree in the MWTM main window, this option is dimmed and cannot be chosen.

Menu Command	Description
Edit > Delete (Delete)	Deletes the currently chosen element or elements from the MWTM database. The MWTM displays the Confirm Deletion dialog box. To: • Delete the chosen elements, click Yes. The items are deleted from the MWTM database and the Confirm Deletion dialog box is closed. • Retain the chosen elements, click No. The items are kept in the MWTM database and the Confirm Deletion dialog box closes. • Prevent the MWTM from displaying the Confirm Deletion dialog box, select the Do not show this again check box. Note If you select the Do not show this again check box, and you later decide you want the MWTM to begin displaying the Confirm Deletion dialog box again, you must select the Confirm Deletions check box in the General GUI settings in the Preferences window. For more information, see the description of the Confirm Deletions check box in Startup/Exit Settings, page 5-4. To permanently delete all elements marked for deletion from the MWTM database, you can also run the mwtm purgedb command (see mwtm purgedb, page B-51). If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Edit > Preferences (Ctrl-H)	Opens the Preferences window.
Network> Node SNMP and Credentials Editor (Alt-S)	Opens the SNMP Configuration dialog box. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Network > Network Discovery (Ctrl-Y)	Opens the Discovery dialog box. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Network > Poll Nodes > Normal Poll (Alt-L)	Polls all chosen nodes. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

Menu Command	Description
Network > Poll Nodes > Clean Poll (Alt-C)	Polls all chosen nodes and removes any Unknown objects after the completion of the poll. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.
Network > Node Archive Management	Opens the Node Archive Management dialog box, allowing you to view archived GTT files, route table files, or MLR address table files and perform various functions on the files. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Network > Node File Management	Opens the Node File Management dialog box, allowing you to view GTT files, route table files, or MLR address table files and perform various functions on the files. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
View > Show Topology (Ctrl-T)	Opens the topology window.
View > MWTM Server > Connect via Telnet (Ctrl+Shift+T)	Opens a Telnet window to the server.
View > MWTM Server > Connect via SSH (Ctrl+Shift+S)	Opens a Secure Shell (SSH) window to the server. Note The key size on the SSH server must be a minimum of 512 bits and a maximum of 2048 bits.
View > MWTM Server > Status	Opens the Server Status Information window.
View > Web > Home	Displays the MWTM web interface home page in a web browser.
View > Web > Administrative	Displays the MWTM web administrative page in a web browser.
View > Web > Reports	Displays the MWTM web reports main page in a web browser.
View > Web > Archived Events > Status Changes	Displays the archived status changes in a web browser.
View > Web > Archived Events > SNMP Traps	Displays the archived SNMP traps in a web browser.
View > Web > Archived Events > Status Changes and SNMP Traps	Displays both the archived status changes and archived SNMP traps in a web browser.
View > Web > Software Versions	Displays the MWTM software versions for the server you are connected to, and which is currently running the MWTM server, in a web browser.
View > Message of the Day	Opens the Message of the Day dialog box.

Menu Command	Description
View > Cisco.com	Displays the Cisco.com Home Page in a web browser.
Go > Back (Alt-Left Arrow) ¹	Navigates back to the last window viewed in this session.
Go > Forward (Alt-Right Arrow) ¹	Navigates forward to the last window viewed in this session.
Go > Back > <i>List of Windows</i>	Navigates back to a window viewed in this session. The MWTM maintains a list of up to 10 Back windows.
Go > Forward > <i>List of Windows</i>	Navigates forward to a window viewed in this session. The MWTM maintains a list of up to 10 Forward windows.
Tools > Route Table > From Archive (Alt-J) (ITP only)	Opens the Load Route Table from Archive wizard. If you select an Unmanaged node, this option is dimmed and cannot be chosen. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Tools > Route Table > From Node (Alt-O) (ITP only)	Opens the Route Table dialog box by using a route table from an ITP node. If you select an Unmanaged node, this option is dimmed and cannot be chosen. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Tools > Route Table > From File (Alt-I) (ITP only)	Opens the Route Table dialog box by using a route table from a file. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Tools > Global Title Translator Editor (Ctrl-G) (ITP only)	Launches the GTT client. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.
Tools > Address Table Editor (Alt-A) (ITP only)	Launches the Address Table Editor, which you use to create new address table files, load existing address table files, perform semantic checks, save address table files, and deploy address table files to an ITP. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

Menu Command	Description
Tools > Event Editor (Alt-B)	Launches the Event Editor, which you use to: • Customize the visible category, severity, color, and message associated with events • Configure sounds for the MWTM to play for different types of events • Load, save, and deploy customized event configurations. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.
Tools > Event Sounds (Ctrl-U)	Opens the Event Sound Filters dialog box, which you use to define sounds that the MWTM client should play when specific events are logged.
Tools > Virtual RAN Backhaul Editor (Ctrl-B)	Launches the Virtual RAN Backhaul Editor, which you use to create a virtual RAN backhaul by grouping real backhauls.
Tools > Launch > CiscoView <machine name> (Ctrl-3)	Launches CiscoView, which provides a real-time, color-coded, graphical representation of Cisco objects. You can use CiscoView to quickly identify an incorrect status on a port or interface. This option is dimmed if the chosen node is: not a recognized node; in Unmanaged status; or has a Device Type of Unknown. (CiscoWorks cannot monitor Unmanaged, Unknown, or unrecognized nodes.) This option is not visible if you did not specify a CiscoWorks server during installation. See the “Installing MWTM on Solaris” and “Installing MWTM on Windows” chapters of the <i>Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1</i> for more information.
Tools > Launch > CiscoWorks LMS Portal <machine name>	Launches CiscoWorks LMS Portal, which provides a dashboard of tools and utilities such as CiscoView, Resource Manager Essentials, Device Center, CSG Service Manager, and GGSN Service Manager.
Tools > Launch > CSG Service Manager ² <machine name> (Ctrl-4)	Launches the CSG Service Manager, which provides provisioning and service activation of CSG features in the network.

Menu Command	Description
Tools > Launch > Device Center <machine name> (Ctrl-2)	Launches the CiscoWorks Device Center, which provides a number of web-based functions, including reachability trends, response time trends, interface status, syslog browsing, and detailed inventory. The MWTM prompts you for a CiscoWorks user ID and password before linking to CiscoWorks. The link to CiscoWorks has these prerequisites. CiscoWorks must: • Be installed somewhere in the network. • Monitor the specific device. This option is dimmed if the chosen node is: not an recognized node; in Unmanaged status; or has a Device Type of Unknown. (CiscoWorks cannot monitor Unmanaged, Unknown, or unrecognized nodes.) This option is not visible if you did not specify a CiscoWorks server during installation. See the “Installing MWTM on Solaris” and “Installing MWTM on Windows” chapters of the <i>Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1</i> for more information.
Tools > Launch > GGSN Service Manager ² <machine name> (Ctrl-5)	Launches the GGSN Service Manager, which provides provisioning and service activation of GGSN features in the network.
Help > Topics (F1)	Displays the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Displays online help for the current window.
Help > About (F3)	Displays build date, version, SSL support, and copyright information about the MWTM application.

1. In the UNIX environment (Solaris or Linux), this key combination can be mapped to a different function based on the Common Desktop Environment (CDE) that a user might have. For example, in Solaris CDE, Alt-Left Arrow and Alt-Right Arrow combinations are typically mapped to move back and forward through the different desktops. To remap the keys for use with the MWTM, see your UNIX Desktop Environment guide.
2. The MWTM attempts to launch the URL of the service manager that resides on the LMS server. If the service manager is not installed on the LMS server, you will receive an HTTP 404 error. To prevent this error, ensure that the service managers are installed on the LMS server, or remove the CSG or GGSN network setting with the **mwtm manage** command.

Using the MWTM Toolbar

The MWTM toolbar appears under the menu bar in the MWTM client windows, and above the navigation tree in the MWTM web interface.

The MWTM toolbar contains:

Element	Description
 Sort tree by name	Sorts all content in the navigation tree alphabetically by name.
 Sort tree by status	Sorts all content in the navigation tree by status, from the highest alarms to the lowest.
 Go back or forward one navigation change	(Only in MWTM client) Click to browse forward or backward in your navigation changes. In the MWTM web interface, click the browser's back and forward buttons.
 Location	Shows your current location in MWTM. Some locations are clickable links to which you can navigate directly.

Accessing the MWTM Through a Web Browser

You can manage network nodes through one of two graphical user interfaces:

- **MWTM client interface**—The standard interface for accessing MWTM data. (This interface is described in [Displaying the MWTM Main Window, page 4-16.](#))
- **MWTM web interface**—A browser interface for accessing MWTM data. (This interface is introduced here and fully described in [Chapter 11, “Accessing Data from the Web Interface.”](#))

A comparison of the GUI features supported in each interface is shown in this matrix:

GUI Features	Web Interface	Client Interface	Notes
Main window	X	X	Slight differences exist between the interfaces (in the navigation tree and content area displays).
Discovery window		X	Client-only feature, but the nodes that appear in the web interface are refreshed after a discovery is performed in the client interface.
Historical Data	X		You enter a start and stop time for the data you are interested in, and the MWTM retrieves the data from its database. You can access the web interface display from the right-click menus in the client interface.
Real-time Data		X	The MWTM periodically polls the node for real-time data, and updates the graphs as new data is received.

GUI Features	Web Interface	Client Interface	Notes
Topology		X	Client-only feature.
High-level editors		X	These editors appear under the Tools menu of the MWTM main window: • Route Table Editor • GTT Title Editor • Address Table Editor • Event Editor
Provisioning	X		Web-only feature for ITP objects. To launch web provisioning from the MWTM client, select the ITP object in the navigation tree and choose the Provision option from the right-click menu.

You access the web interface using one of two methods:

- Open a browser and enter **http://server_name:1774** in the Address field.
- From the MWTM client interface, choose **View > Web > Home**.

The web interface window opens in the browser window as shown in [Figure 4-1](#).

For detailed information about the MWTM web interface, see [Chapter 11, “Accessing Data from the Web Interface.”](#)

Loading and Saving MWTM Files

You use the MWTM to quickly and easily load and save MWTM files. The files are on the MWTM server and you can load them on any connected MWTM client.

To display a Load File dialog box, use one of these procedures:

Launched From	Choose	Window Launched	Notes
Address Table Editor (ITP only)	File > Load > Load from File	Load File Dialog: Address Table File List	See Loading an Existing Address Table File , page 15-8.
Discovery dialog box	File > Load Seeds	Load File Dialog: Seed File List	See Loading Seed Nodes and Seed Files , page 4-7.
Event Filter dialog box	Load	Load File Dialog: Load Filter	See Loading an Existing Filter , page 9-25.
GTT Editor (ITP only)	File > Load	Load File Dialog: GTT File List	See Loading an Existing GTT File , page 14-31.
Preferences window	File > Load System Default Prefs	None	See Displaying the Preferences Menu , page 5-3.

Launched From	Choose	Window Launched	Notes
Route Table dialog box (ITP only)	File > Load	Load File Dialog: Route Table File List	See Loading an Existing Route Table File , page 13-12.
View Editor window	File > Load	Load File Dialog: View List	See Loading a Client-Specific View , page 7-15.

**Note**

To load the DEFAULT network view, choose **File > Load DEFAULT View** from the MWTM main menu. The MWTM loads the DEFAULT view.

To display a Save File dialog box, use one of these procedures:

Launched From	Choose	Window Launched	Notes
Address Table Editor (ITP only)	File > Save As	Save File Dialog: Address Table File List	See Saving an Address Table File , page 15-23.
Discovery dialog box	File > Save As	Save File Dialog: Seed File List	See Saving a Seed File , page 4-8.
Event Filter dialog box	File > Save As	Save File Dialog: Save Filter	See Saving a Filter File , page 9-26.
GTT Editor (ITP only)	File > Save As	Save File Dialog: GTT File List	See Saving a GTT File , page 14-42.
Route Table dialog box (ITP only)	File > Save As	Save File Dialog: Route Table File List	See Saving a Route Table File , page 13-13.
View Editor window	File > Save As	Save File Dialog: View List	See Closing the View Editor Window , page 7-14.

Using the Windows Start Menu

This section includes:

- [Changing the Default MWTM Server Name](#), page 4-31
- [Launching the MWTM Client](#), page 4-31
- [Launching the MWTM DOS Prompt](#), page 4-31
- [Launching the MWTM Event Editor](#), page 4-31
- [Launching the MWTM SSL Certificate Tool](#), page 4-32
- [Displaying the MWTM README File](#), page 4-32
- [Uninstalling the MWTM](#), page 4-32

Changing the Default MWTM Server Name

If the IP address or hostname to which your MWTM client is bound fails, you can change the default MWTM server name from the Windows Start menu.

To change the default MWTM server name:

-
- Step 1** Close all open MWTM windows.
- Step 2** Choose **Start > Programs > Cisco MWTM Client > Modify Default MWTM Server Name**. The MWTM opens a DOS window, and asks you to enter the name of the new default MWTM server.
- Step 3** Type the name of the new default MWTM server, and press **Enter**. The MWTM sets the default server to the new name that you entered.
-

**Tip**

See [Connecting to a New Server, page 5-43](#) for more information about changing the default MWTM server name.

Launching the MWTM Client

To launch the MWTM Client, choose **Start > Programs > Cisco MWTM Client > MWTM Client** from the Windows Start menu, or double-click the MWTM icon on the desktop. The MWTM launches the MWTM Client.

Launching the MWTM DOS Prompt

To launch a DOS prompt for the MWTM from the Windows Start menu, choose **Start > Programs > Cisco MWTM Client > MWTM DOS Prompt**. The MWTM opens a DOS window, starting in the *\bin* directory:

- If you installed the MWTM client in the default directory, *C:\Program Files*, then the DOS prompt starts at *C:\Program Files\MWTMClient\bin*.
- If you installed the MWTM client in a different directory, then the *\bin* directory is located in that directory.

Launching the MWTM Event Editor

To launch the MWTM Event Editor, choose **Start > Programs > Cisco MWTM Client > Launch MWTM Event Editor** from the Windows Start menu. The MWTM launches the MWTM Event Editor.

**Note**

The MWTM Event Editor is available to power users (level 2) and higher.

Launching the MWTM SSL Certificate Tool

To launch the MWTM SSL Certificate Tool from the Windows Start menu, choose **Start > Programs > Cisco MWTM Client > MWTM SSL Certificate Tool**.

Displaying the MWTM README File

The MWTM README file contains late-breaking information about the MWTM that might not be found in the other product documentation. To open the MWTM README file from the Windows Start menu, choose **Start > Programs > Cisco MWTM Client > Readme**.

Uninstalling the MWTM

You can uninstall the MWTM from the Windows Start menu. For details, see the “Uninstalling the MWTM Client” section of the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.

Exiting the MWTM Client

When you are finished monitoring network performance statistics, you can exit the MWTM client:

-
Step 1	From the MWTM main menu, choose File > Exit . The Exit MWTM confirmation window appears.
Step 2	Click Yes to close the MWTM client application.
-



CHAPTER 5

Basic Operations

This chapter provides information about basic operations that you can perform in the Cisco Mobile Wireless Transport Manager (MWTM), and contains:

- [Changing Client and Web Preference Settings, page 5-1](#)
- [Viewing Online Help, page 5-22](#)
- [Finding Information in a Window, page 5-23](#)
- [Navigating Table Columns, page 5-24](#)
- [Printing Windows, page 5-25](#)
- [Managing and Deploying ITP Files, page 5-25](#)
- [Exporting Data, page 5-38](#)
- [Integrating the MWTM with Other Products, page 5-39](#)
- [Running Simultaneous Client Sessions, page 5-43](#)
- [Performing Basic Server Operations, page 5-43](#)
- [Using the Command Line Interface, page 5-47](#)



Note

The default directory for installing the MWTM is */opt*. In commands that call for the default directory, if you installed the MWTM in a different directory, you must specify that directory instead of */opt*.

Changing Client and Web Preference Settings

This section contains this information:

- [Changing Client Preference Settings, page 5-2](#)
- [Changing Web Preference Settings, page 5-20](#)
- [Changing Real-Time Poller and Counter Settings, page 5-21](#)

Changing Client Preference Settings

When a user changes some aspect of the MWTM client, such as the size of a window, or the order of columns in a window, the MWTM makes note of the user's preferences on the MWTM client and server. The MWTM saves the user's preferences to the MWTM server when the MWTM client exits.

Thereafter, whenever the user launches the MWTM client, the MWTM searches for the user's preferences. If the MWTM finds the user's preferences on the MWTM server, the MWTM launches the MWTM client with those preferences. Otherwise, the MWTM launches the MWTM client with the default preferences file.

In addition to the user preferences that the MWTM automatically saves, you use the MWTM to change many GUI, data, topology, and table settings that affect the way the MWTM presents its information.

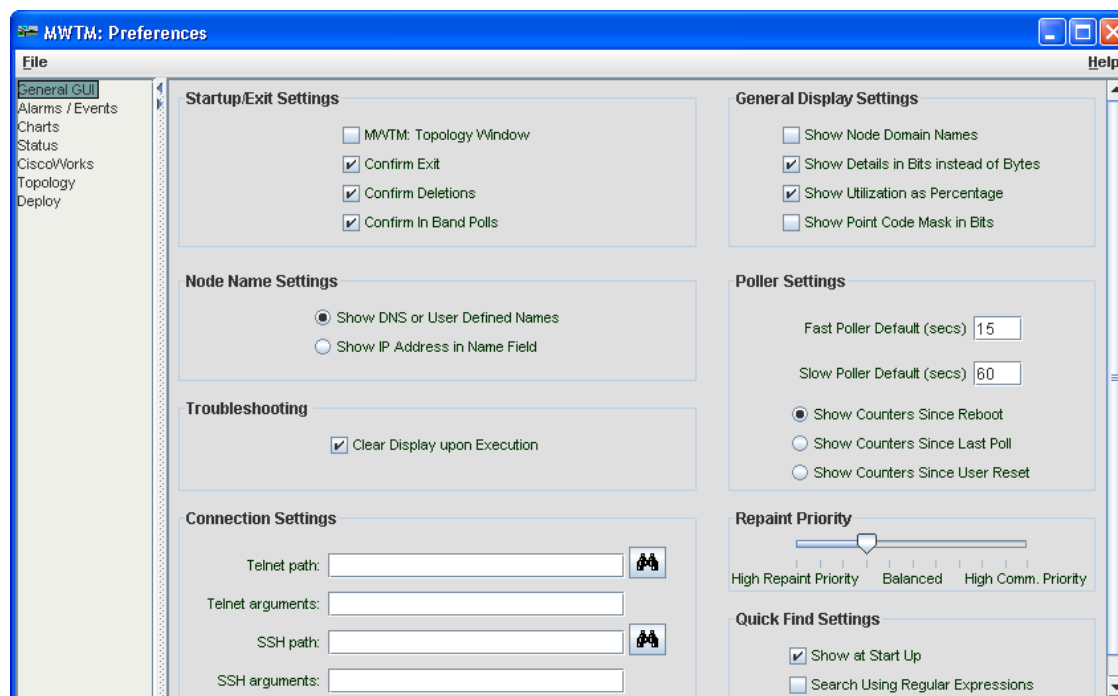


Note

Anyone who uses the MWTM client can change its preference settings, and the changes affect all views running on this client.

To change overall MWTM preference settings, choose **Edit > Preferences** from the MWTM client main menu. The MWTM displays the Preferences window.

Figure 5-1 Preferences Window (Client)



In the Preferences window, you can:

- [Displaying the Preferences Menu, page 5-3](#)
- [Changing General GUI Settings, page 5-4](#)
- [Changing Alarm and Event Settings, page 5-8](#)
- [Changing Charts Settings, page 5-11](#)
- [Changing Status Settings, page 5-12](#)
- [Changing CiscoWorks Server Settings, page 5-13](#)
- [Changing Topology Settings, page 5-14](#)
- [Changing Deploy Settings, page 5-16](#)
- [Customizing Colors, page 5-18](#)
- [Restoring Default Preference Settings, page 5-19](#)

Displaying the Preferences Menu

The menu on the Preferences window contains:

Option	Description
File > Load System Default Prefs	Restores all preference settings to the original system default settings.
File > Save (Ctrl-S)	Saves the preference changes.
File > Close (Ctrl-W)	Closes the Preferences window. To close the Preferences window at any time, choose File > Close. If you have changed any preferences, the MWTM asks if you want to apply the changes before leaving the window: • Click Yes to apply the changes and close the prompt window and the Preferences window. • Click No to close the prompt window and the Preferences window without applying or saving any changes. • Click Cancel to close the prompt window without applying any changes. The Preferences window remains open.
Help > Topics (F1)	Displays the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Displays online help for the current window.
Help > About (F3)	Displays build date, version, SSL support, and copyright information about the MWTM application.

Changing General GUI Settings

You use the General GUI settings in the Preferences window to change general display settings for the MWTM, including which window to display first when starting the MWTM, and whether to display values in bits or bytes.

To display the General GUI settings, choose General GUI in the left pane of the Preferences window.

In the General GUI area you can change:

- [Startup/Exit Settings, page 5-4](#)
- [General Display Settings, page 5-4](#)
- [Node Name Settings, page 5-5](#)
- [Poller Settings, page 5-6](#)
- [Troubleshooting, page 5-6](#)
- [Connection Settings, page 5-7](#)
- [Repaint Priority, page 5-7](#)

Startup/Exit Settings

Use the Startup/Exit Settings pane of the General GUI settings to specify whether you want to display the topology window when you launch the MWTM client, and whether you want the MWTM to prompt you for confirmation when you exit the MWTM client.

The Startup/Exit Settings pane contains:

Check Box	Description
MWTM: Topology Window	If checked, causes the topology window to appear when you start the MWTM. The default setting for this check box is unchecked.
Confirm Exit	If checked, the MWTM prompts you for confirmation when you exit the MWTM client. The default setting for this check box is checked.
Confirm Deletes	If checked, the MWTM prompts you for confirmation when you delete an object. The default setting for this check box is checked. Note If you check the Do not show this again check box in a Confirm Deletion dialog box, and you later decide that you do want the MWTM to display the Confirm Deletion dialog box, you must check the Confirm Deletions check box.
Confirm In Band Polls	If checked, the MWTM prompts you for confirmation when you access a function that requires the MWTM to perform in-band polling of the object.

General Display Settings

Use the General Display pane of the General GUI settings to specify whether the MWTM should:

- Display node domain names.
- Show details in bits instead of bytes.
- Show receive and send utilizations as percentages.
- Show the point code mask in bits instead of dotted notation.

The General Display pane contains:

Check Box	Description
Show Node Domain Names	If checked, the MWTM shows node domain names in its displays. The default setting for this check box is unchecked (do not show node domain names).
Show Details in Bits Instead of Bytes	If checked, the MWTM displays data and data rates in bits instead of bytes: • Check if you want the MWTM to display data in bits, and data rates in bits per second. This is the default setting. • Uncheck if you want the MWTM to display data in bytes, and data rates in bytes per second.
Show Utilization as Percentage	If checked, the MWTM displays receive and send utilization for linksets and links as a percentage: • Check if you want the MWTM to display utilization as a percentage. This is the default setting. • Uncheck if you want the MWTM to display utilization in Erlangs.
Show Point Code Mask in Bits (ITP only)	If checked, the MWTM displays point code masks as a number of bits instead of dotted-decimal format. The MWTM applies this setting to all point code masks in the MWTM client, including those in the Route Table dialog box, in messages, and so on. • Uncheck if you want the MWTM to display point code masks in dotted-decimal format (octets separated by periods). This is the default setting. • Check if you want the MWTM to display point code masks as a number of bits. For more information about point code masks, see Route Table, page 13-8 .

Node Name Settings

Use the Node Name pane of the General GUI settings to specify how the MWTM should display node names.

The Node Name pane contains these radio buttons:

Radio Buttons	Description
Show DNS or User Defined Names	Indicates whether the MWTM should identify nodes by their DNS or user-defined names. The default setting for this radio button is clicked.
Show IP Address in Name Field	Radio button used to indicate whether the MWTM should identify nodes by their IP addresses. The default setting for this radio button is unclicked.

Poller Settings

Use the Poller pane of the General GUI settings to change the MWTM poller and counter settings. The Poller pane contains:

Field or Radio Button	Description
Fast Poller Default (secs)	Default interval, in seconds, for the fast poller. The valid range is 5 to 60 seconds. The default setting is 15 seconds. The fast poller appears in these MWTM client windows: • MWTM Real-Time Statistics: CPU Statistics window • (ITP only) Details window for an Application Server • (ITP only) Details window for a Linkset • (ITP only) Details window for a Signaling Gateway Mated Pair You can change the valid range and default setting in the <i>Server.properties</i> file. For more information, see Changing MWTM Server Poller Settings, page 3-2.
Slow Poller Default (secs)	Default interval, in seconds, for the slow poller. The valid range is 60 seconds to 300 seconds. The default setting is 60 seconds. The slow poller is used in all the MWTM client windows except those listed previously that use the fast poller. Note You can change the valid range and default setting in the <i>Server.properties</i> file. For more information, see Changing MWTM Server Poller Settings, page 3-2.
Show Counters Since Reboot	Radio button used to configure the MWTM client to clear all counters in MWTM web pages whenever the node reboots. The default setting for this radio button is clicked.
Show Counters Since Last Poll	Radio button used to configure the MWTM client to clear all counters whenever an MWTM web page is polled. The default setting for this radio button is unclicked.
Show Counters Since User Reset	Radio button used to configure the MWTM client to clear all MWTM counters whenever the user resets the counters on an MWTM web page. The default setting for this radio button is unclicked.

Troubleshooting

Use the Troubleshooting pane of the General GUI settings to specify whether the MWTM clears the display window upon command execution.

The Troubleshooting pane contains:

Field	Description
Clear Display upon Execution	Clears the output display each time you execute a command.

Connection Settings

Use the Connection Settings pane of the General GUI settings to set the Telnet or SSH path and arguments for accessing nodes using one of these methods.



Note

To connect to a node using SSH, the key size on the node must be configured to a minimum of 768 bits and a maximum of 2048 bits.

The Connection Settings pane contains:

Field	Description
Telnet path	Use to modify the default MWTM Telnet path to an executable file (for example, <i>putty.exe</i>). Click Find to choose a Telnet path on your local machine. Note Choosing a non-GUI file might not yield the expected results.
Telnet arguments	Optional arguments that the MWTM passes to the Telnet executable when the MWTM invokes it. For example, to set the host name and port number for the connection, specify -telnet \$host \$port . ¹
SSH path	Use to modify the default MWTM SSH path to an executable file (for example, <i>putty.exe</i>). Click Find to choose an SSH path on your local machine. Note Choosing a non-GUI file may not yield the expected results.
SSH arguments	Optional arguments that the MWTM passes to the SSH executable when the MWTM invokes it. For example, to set the host name and port number for the connection, specify -ssh \$host \$port . ¹

1. When you right-click a node in the navigation tree and choose Connect To, the variables \$host and \$port are replaced with the host name and port number of the node.

Repaint Priority

Use the Repaint Priority pane of the General GUI settings to balance the responsiveness versus efficiency of the MWTM client. This setting controls how quickly the MWTM client repaints its displays.

The Repaint Priority pane contains a sliding control: 

Field	Description
Repaint Priority	Balances the MWTM client's responsiveness versus efficiency. The valid range is 0 through 10, with 0 representing a high repaint priority (high responsiveness, low efficiency) and 10 representing a high communication priority (high efficiency, low responsiveness): • To maximize repainting (responsiveness) over communication (efficiency), slide the selector toward High Repaint Priority. • To maximize communication (efficiency) over repainting (responsiveness), slide the selector toward High Comm. Priority. • The default setting is 2 (the third mark from the left).

Changing Alarm and Event Settings

Use the Alarms / Events settings in the Preferences window to:

- Change the default background color for each type of alarm or event
- Specify whether to display acknowledged alarms or events
- Specify the types of events the MWTM should display in the alarms and events tables, including the:
 - Category and severity
 - Whether the event is acknowledged
 - Other properties

To display the preference settings for alarms and events, select Alarms / Events in the left pane of the Preferences window.

In the right pane you can change:

- [Colors, page 5-8](#)
- [Alarm-specific Colors, page 5-8](#)
- [Time Format, page 5-9](#)
- [Date Format, page 5-9](#)
- [Categories, page 5-9](#)
- [Severities, page 5-10](#)
- [Other, page 5-11](#)

Colors

The Alarm / Event Colors pane contains:

Field	Description
Change Color	Opens the Select Event Color dialog box from which you select a color for an alarm or event type. For more details, see Customizing Colors, page 5-18 .
Critical	Indicates the background color for Critical alarms or events. The default is red.
Major	Indicates the background color for Major alarms or events. The default is orange.
Minor	Indicates the background color for Minor alarms or events. The default is yellow.
Warning	Indicates the background color for Warning alarms or events. The default is blue.
Informational	Indicates the background color for Informational alarms or events. The default is white.
Indeterminate	Indicates the background color for Indeterminate alarms or events. The default is cyan.
Normal	Indicates the background color for Normal alarms or events. The default is light green.

Alarm-specific Colors

The Alarm-specific Colors pane contains:

Field	Description
Change Color	Opens the Select Event Color dialog box from which you select a color for alarms and events of unmanaged objects. For more details, see Customizing Colors, page 5-18 .
Unmanaged	Indicates the background color for unmanaged alarms or events. The default is gray.

Time Format

The Time Format pane contains:

Button	Description
12 Hour	Click this radio button to configure alarm or event time stamps to use 12-hour format (for example, 07:10:09).
24 Hour	Click this radio button to configure alarm or event time stamps to use 24-hour format (for example, 19:10:09).

Date Format

The Date Format pane contains:

Button	Description
Month-First	Click this radio button to configure alarm or event date stamps with the month appearing first (for example, 8/16/05).
Day-First	Click this radio button to configure alarm or event date stamps with the day appearing first (for example, 16/8/05).

Categories

In the Categories pane, you specify which event categories to display in the Event History window.

The Categories pane contains:

Field or Button	Description
Status	Indicates whether Status events should appear in the Event History window. The default is checked.
Trap	Indicates whether Trap events should appear in the Event History window. The default is checked.
Create	Indicates whether Create events should appear in the Event History window. The default is checked.
Delete	Indicates whether Delete events should appear in the Event History window. The default is checked.
Discover	Indicates whether Discover events should appear in the Event History window. The default is checked.

Field or Button	Description
Edit	Indicates whether Edit events should appear in the Event History window. The default is checked.
Ignore	Indicates whether Ignore events should appear in the Event History window. The default is checked.
Login	Indicates whether Login events should appear in the Event History window. The default is checked.
LoginDisable	Indicates whether LoginDisable events should appear in the Event History window. The default is checked.
LoginFail	Indicates whether LoginFail events should appear in the Event History window. The default is checked.
Logout	Indicates whether Logout events should appear in the Event History window. The default is checked.
OverWrite	Indicates whether OverWrite events should appear in the Event History window. The default is checked.
Poll	Indicates whether Poll events should appear in the Event History window. The default is checked.
Purge	Indicates whether Purge events should appear in the Event History window. The default is checked.
Select All	Checks all event category check boxes.
Deselect All	Unchecks all event category check boxes.

**Note**

The fields in the previous table are default categories; however, the MWTM system administrator might define additional categories. For information about custom categories, see [Changing Event Categories, page 9-41](#).

Severities

In the Severities pane, you specify which alarm or event severities to display in the Event History and Active Alarms windows.

The Severities pane contains these default fields:

Field	Description
Critical	Indicates whether alarms and events of severity Critical should appear in the window. The default is checked.
Major	Indicates whether alarms and events of severity Major should appear in the window. The default is checked.
Minor	Indicates whether alarms and events of severity Minor should appear in the window. The default is checked.
Warning	Indicates whether alarms and events of severity Warning should appear in the window. The default is checked.

Field	Description
Informational	Indicates whether alarms and events of severity Informational should appear in the window. The default is checked.
Indeterminate	Indicates whether alarms and events of severity Indeterminate should appear in the window. The default is checked.
Normal	Indicates whether alarms and events of severity Normal should appear in the window. The default is checked.

Other

Use the Other pane to further define the filter for the Event History and Active Alarms windows. These settings apply to all event displays in the current view.

The Other pane contains:

Check Box or Field	Description
Acknowledged	Indicates whether only acknowledged alarms and events should appear in the window. The default is checked.
Unacknowledged	Indicates whether only unacknowledged alarms and events should appear in the window. The default is checked.
Time Before	Indicates whether only alarms and events that the MWTM logs prior to a specified date and time should appear in the window. The default is checked.
Time Before Field	Specifies the date and time prior to which alarms and events that the MWTM logs should appear in the window. This field is dimmed unless the Time Before check box is checked.
Time After	Indicates whether only alarms and events that the MWTM logs after a specified date and time should appear in the window. The default is checked.
Time After Field	Specifies the date and time after which alarms and events that the MWTM logs should appear in the window. This field is dimmed unless the Time After check box is checked.
Message Contains	Indicates whether only alarms and events that contain the specified message text should appear in the window. The default is checked.
Match Case	Indicates whether only alarms and events that match the case of the text in the Message Contains field should appear in the window. This field is dimmed unless the Message Contains check box is checked. If the Message Contains check box is checked, the default setting for this check box is checked.
Suppress Events for unmanaged nodes	Suppresses all alarms and events from nodes that are unmanaged. The default setting for this check box is unchecked.

Changing Charts Settings

Use the Charts pane in the Preferences window to change default settings for the elements in real-time data charts for application servers, application server process associations, links, and linksets.

To display the Charts pane, click **Charts** in the left pane of the Preferences window.

The Charts pane contains:

Field or Button	Description
Series	Indicates the time series being defined. A time series is a set of data collected sequentially at a fixed interval of time. The default values for series are: - Series 0: Dot, Solid, Red - Series 1: Box, Solid, Green - Series 2: Triangle, Solid, Blue - Series 3: Diamond, Solid, Black - Series 4: Star, Solid, Pink - Series 5: Cross, Solid, Orange - Series 6: Circle, Solid, Gray - Series 7: Square, Solid, Light Green - Series 8: Vertical Line, Solid, Red - Series 9: Horizontal Line, Solid, Green - Series 10: Dot, Solid, Blue - Series 11: Box, Solid, Black - Series 12: Triangle, Solid, Pink - Series 13: Diamond, Solid, Orange - Series 14: Star, Solid, Gray - Series 15: Cross, Solid, Light Green - Series 16: Circle, Solid, Red
Symbol Style	Drop-down list box used to define the symbol associated with a series. To change the symbol for a series, select a new value: Dot, Box, Triangle, Diamond, Star, Vertical Bar, Horizontal Line, Cross, or Circle.
Line Style	Drop-down list box that you use to define the style of line that connects data points in the chart. To change the line style for a series, select a new value: Solid, Long Dash, Long-Short-Long (LSL) Dash, Short Dash, Dash Dot, or None.
Color	Indicates the current color for the series.
Change Color	Opens the Select Series Color dialog box in which you select a color for a series. For more details, see Customizing Colors, page 5-18 .

Changing Status Settings

You use the MWTM to customize the sort order for status settings, as well as the color of each status setting.

When you change the sort order or the color of a status setting, most MWTM client windows reflect the new sort order or color immediately. All other windows reflect the new sort order or color at the next poll.

When you change the color of a status, most MWTM client windows reflect the new color immediately. All other windows reflect the new color at the next poll.

To display the Status settings, click **Status** in the left pane of the Preferences window.

The Status pane contains:

Field or Button	Description
Status Sort Order	Indicates the status setting being defined. The default status sort order and colors are: • None: Black • Unknown: Red • Unavailable: Red • Inactive: Red • Failed: Red • Down: Red • Blocked: Red • Pending: Red • Warning: Yellow • Shutdown: Blue • Inhibited: Blue • InhibitLoc: Blue • InhibitRem: Blue
Status Sort Order (continued)	• Discovering: Cyan • Polling: Cyan • Waiting: Gray • Unmanaged: Gray • Active: Green
Move Up	Moves the chosen status setting up in the Status Sort Order list.
Change Color	Opens the Select Status Color dialog box in which you select a color for a status. For more details, see Customizing Colors, page 5-18 .
Move Down	Moves the chosen status setting down in the Status Sort Order list.
Reset Order	Restores the status settings to the default sort order.
Reset Colors	Restores the status settings to the default colors.

Changing CiscoWorks Server Settings

You can configure the CiscoWorks server name and port numbers for all connected MWTM clients:

- During MWTM installation. See the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.
- After installation by running the **mwtm cwsetup** command. See [mwtm cwsetup, page B-21](#).

All clients connected to the MWTM server retain the CiscoWorks settings that were made during installation or the last time you ran the **mwtm cwsetup** command. However, you can overwrite the CiscoWorks settings for a particular client by using the preferences window.

To change the CiscoWorks server settings for a particular client:

Step 1 From the main window, choose **Edit > Preferences > CiscoWorks**.

Step 2 Click **CiscoWorks** in the left pane of the Preferences window.

The CiscoWorks server settings contain:

Check Box or Field	Description
IP Address or DNS Host Name ¹	The IP address or the DNS host name of the CiscoWorks server.
Port ¹	The access port on the CiscoWorks server. The default setting is 1741.
Secure Port ¹	The port number on the CiscoWorks server that is used for secure access, for example, SSL access. The default setting is 443.
Secure Connection	Indicates if the connection to the CiscoWorks server is secure.

1. Changing this setting affects only the MWTM client you are using. All other MWTM clients retain the CiscoWorks settings that were made during installation or the last time you ran the **mwtm cwsetup** command.

Step 3 From the Preferences window menu bar, choose **File > Save**.



Note

To do this procedure from the MWTM web interface, see [Changing Web Preference Settings, page 5-20](#).

Changing Topology Settings

Use the Topology pane in the Preferences window to change default settings for the topology window.

To display the topology settings, select Topology in the left pane of the Preferences window.

The Topology pane contains:

Check Box or Field	Description
Spring Layout Spacing Factor (1-10)	Indicates how far to space nodes when the MWTM draws the Spring Layout topology map. Valid values are 1 through 10, with 1 being closer together and 10 being farther apart. The default spacing factor is 5. Even if you apply preferences and close the Preferences window, the topology map does not show the new spacing factor until you choose Topology Tools > Layout > Spring , or click the Spring Layout button.
Show Mouse Overs	Specifies whether tooltips are enabled in topology maps. Checked is the default.

Check Box or Field	Description
Draw Connections When Dragging a Node	Specifies whether the MWTM draws connection lines in the topology map as you move nodes: • Check if you want the MWTM to draw the associated connection lines dynamically as you move a node. • Uncheck if you do not want the MWTM to draw the associated connection lines until after you have finished moving a node. Unchecked is the default.
Show Small SS7 Icons (ITP only)	Specifies the size of the SS7 icons in the topology map: • Uncheck if you want the MWTM to display large SS7 icons. Unchecked is the default. • Check if you want the MWTM to display small SS7 icons. This setting can save space in the topology map, making it easier to read.
Show Non-ITP Nodes (ITP only)	Specifies whether the MWTM should display non-ITP nodes and linksets in the topology map: • Check if you want the MWTM to display non-ITP nodes and linksets in the topology map. Checked is the default. • Uncheck if you want the MWTM to hide non-ITP nodes and linksets in the topology map. (The navigation tree still shows the hidden signaling points and linksets.)
Show Point Code and Node Name (ITP only)	Specifies whether the MWTM should display point codes as well as node names in the topology map: • Uncheck if you want the MWTM to display point codes but not node names. Unchecked is the default. • Check if you want the MWTM to display both point codes and node names.
X Performance Enhancer (AntiAliasing Off)	Specifies whether antialiasing is turned on in the topology map. Antialiasing, which is on by default, improves the appearance of the icons and connections in the map. However, antialiasing can impact the performance of the MWTM client on a remote workstation (that is, a Solaris or Linux workstation by using xhost, or a Windows workstation using an X-Window system emulator such as eXceed or Reflection X). • Uncheck if you want to turn on antialiasing in the topology map. Unchecked is the default. • Check if you want to turn off antialiasing. Remember that performance is always better if you access the MWTM by installing the MWTM client on the remote workstation.

Changing Deploy Settings


Note

Deploy settings are only for ITP networks. If you configure the MWTM to manage ITP networks, the deploy settings will appear in the Preferences window. You customize the MWTM to manage ITP networks during installation. You can also do this later by command (see [mwtm manage](#), page B-40).

Use the Deploy settings to change the way the Deployment Wizard works.

To display the Deploy settings, select Deploy in the left pane of the Preferences window.

The Deploy settings contain:

Check Box or Field	Description
Turn On Term Monitor During File Activation	Indicates whether the MWTM should turn on the terminal monitor before activating a route table file or GTT file on the ITP, and turn it off after activation (whether or not the activation was successful). If you turn on the terminal monitor during activation, detailed activation error messages appear in the connection log. These messages can be useful if activation fails. However, all node console logging messages also appear in the connection log; so, many nonactivation messages might also appear. The default is checked.
Turn Off All Debug Output Before Turning On Term Monitor	Indicates whether debug messages should appear in the connection log. The default is checked. If you check the Turn On Term Monitor During File Activation check box, all node console logging messages appear, including all debug messages that are currently enabled on the node.
Turn Off All Debug Output Before Turning On Term Monitor (continued)	You can then check the Turn Off All Debug Output Before Turning On Term Monitor check box to turn off all debug messages. This setting can reduce the number of nonactivation messages in the connection log. The default is checked. Note The MWTM does not turn the debug messages back on after activation. Ensure that other users are not debugging on the node before checking this check box. This check box is dimmed unless you check the Turn On Term Monitor During File Activation check box.
Synchronize Active and Standby Storage If Node Is Configured as Redundancy Mode	Cisco 7507, 7513, and 7600 series routers support redundancy, which requires synchronization of the active and all standby storage devices. If you want the MWTM to use a node's <i>configured</i> redundancy mode to determine whether the MWTM should replicate storage operations (such as creating files, uploading, deleting, and so on) among the active and all standby storage devices, click this radio button. Note This radio button is mutually exclusive with the Synchronize Active and Standby Storage If Node Is Operating in Redundancy Mode and Do Not Synchronize Active and Standby Storage radio buttons.

Check Box or Field	Description
Synchronize Active and Standby Storage If Node Is Operating in Redundancy Mode	If you want the MWTM to use a node's <i>operating</i> redundancy mode to determine whether the MWTM should replicate storage operations (such as creating files, uploading, deleting, and so on) among the active and all standby storage devices, in the right pane click this radio button. The default is clicked. Note This radio button is mutually exclusive with the Synchronize Active and Standby Storage If Node Is Configured as Redundancy Mode and Do Not Synchronize Active and Standby Storage radio buttons.
Do Not Synchronize Active and Standby Storage	If you want the MWTM to perform storage operations only on the active storage device (that is, no automatic synchronization of active and standby storage devices), click this radio button. Clicking this radio button requires you to manually synchronize the active and standby storage devices. This radio button is mutually exclusive with these radio buttons: - Synchronize Active and Standby Storage If ITP Is Configured as Redundancy Mode - Synchronize Active and Standby Storage If ITP Is Operating in Redundancy Mode
Enable Auto Refresh Node Storage In Node File Management Dialog	Indicates whether the Node File Management dialog box should refresh storage device content automatically at user-defined intervals. Clicking this check box enables the Node File Management dialog box to detect any updates made to the file system. In addition, you can configure the node to disconnect idle connection sessions. If you check this check box, the MWTM automatically generates node operations at the user-defined interval, which prevents disconnection of the session by the node. The default is unchecked. To enable the automatic refresh, check this check box, then specify a Refresh Interval. The valid range is 1 seconds to an unlimited number of seconds. The default interval is 60 seconds.
Always Overwrite Existing File In Deployment Wizard	Indicates whether the Deployment Wizard should overwrite an existing file with the same filename automatically, without prompting the user. The default is unchecked.
Always Skip Archive Comments	Indicates whether the Deployment Wizard should skip archive comments. The default is unchecked. This check box appears only if deploy comments are set to optional. For details, see mwtm deploycomments, page B-95. If deploy comments are set to required, this check box does not appear.

Check Box or Field	Description
Always Activate Deployed File In Deployment Wizard	Indicates whether the Deployment Wizard should activate the deployed file automatically, without prompting the user. The default is unchecked.
Command Timeout in Seconds	Indicates how long, in seconds, an MWTM client with a session to a node should wait for a response from the node before closing the session. The valid range is 1 second to an unlimited number of seconds. The default is 90 seconds.

Customizing Colors

You use the MWTM to customize the colors for these settings:

Setting	Menu Selection	Color Dialog
Alarm or event severity	Click Alarms / Events in the left pane of the Preferences window (Figure 5-1), then click Change Color in the Alarm / Event Colors section.	Select Event Color
Series in real-time charts	Click Charts in the left pane of the Preferences window (Figure 5-1), then click Change Color in the Series Colors section.	Select Series Color
Status	Click Status in the left pane of the Preferences window (Figure 5-1), select a status setting, then click Change Color .	Select Status Color

The Select Color dialog box contains:

- [Swatches Tab \(Recommended\)](#), page 5-18
- [HSB Tab](#), page 5-19
- [RGB Tab](#), page 5-19
- [Select Color Field and Buttons](#), page 5-19

Related Topics:

- [Changing Alarm and Event Settings](#), page 5-8
- [Changing Charts Settings](#), page 5-11
- [Changing Status Settings](#), page 5-12

Swatches Tab (Recommended)

You use the Swatches tab of the Select Color dialog box to select a color from a set of color swatches. This is the recommended method for selecting a color.

To display the Swatches tab, click the **Swatches** tab in the Select Color dialog box.

To select a color, select a swatch. The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

HSB Tab

You must also choose hue, saturation, and brightness (HSB) variables to select a color.

To display the HSB tab, click the **HSB** tab in the Select Color dialog box.

To select a color, you can either:

- Select a color range on the vertical color bar, then select a specific color by moving the cursor around on the color square.
- Enter specific values in the (hue), S (saturation), and B (brightness) fields.

The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

RGB Tab

You then select the red, green, and blue (RGB) content of the color.

To display the RGB tab, click the **RGB** tab in the Select Color dialog box.

To select a color, select values for the Red, Green, and Blue fields. The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

Select Color Field and Buttons

The Select Color dialog box contains:

Field or Button	Description
Preview	Displays a preview of the current chosen color. Whichever method you choose to select a color, the chosen color appears in the Preview field. When you are satisfied with the color, click OK .
OK	Sets the color as shown in the Preview field, and closes the Color dialog box.
Cancel	Closes the Color dialog box without selecting a color.
Reset	Resets the color to its initial setting.

Restoring Default Preference Settings

If you decide you do not like your modified preference settings, you can use the MWTM to restore all preference settings to the original system default settings. To do so:

-
- Step 1** Display the Preferences window, as described in [Changing Client Preference Settings, page 5-2](#).
- Step 2** Choose the **File > Load System Default Prefs** menu option.
- The MWTM restores the default settings.
-

Changing Web Preference Settings

Access the web preference settings by clicking the Preferences link in the title bar of any web interface window. Web preferences include a subset of the preferences that are available in the client interface.

To change web preferences settings:

-
- Step 1** Click **Preferences** in the title bar of any MWTM web page.
- Step 2** In the Preferences window, to display the:
- a. General GUI settings, click the **General GUI** tab.
 - b. CiscoWorks server settings, click the **CiscoWorks** tab.
- Step 3** Change the settings you want to modify (refer to the table following this procedure for descriptions of the settings). If you enter a new value in a text field, press **Enter** or **Tab** to activate the change.



Note

For any user, common preferences between the web and client interfaces are shared. However, if the web and client interfaces are active at the same time, and you exit the client interface, any changes you made to the web preferences are overwritten by the client preferences.

You can now exit the web preferences window.

The Web Preferences window contains:

Check Box, Radio Button, or Field	Description
General GUI tab	
Show DNS or User-Defined Names	Indicates whether the MWTM should identify nodes by their DNS or user-defined names. The default setting for this radio button is clicked.
Show IP Address in Name Field	Indicates whether the MWTM should identify nodes by their IP addresses. The default setting for this radio button is unclicked.
Show Node Domain Names	If checked, the MWTM shows node domain names in its displays. The default setting for this check box is unchecked (do not show node domain names).
Clear Display upon Execution	Clears the output display each time you execute a command.
Slow Poller Interval (secs)	Default interval, in seconds, for the slow poller. The valid range is 60 seconds to 300 seconds. The default setting is 60 seconds. Note You can change the valid range and default setting in the <i>Server.properties</i> file. For more information, see Changing MWTM Server Poller Settings, page 3-2 .
Status Refresh Interval (secs)	Specifies the default setting for how frequently the MWTM refreshes the web pages on the web interface. The valid range is 180 seconds to 900 seconds. The default setting is 180 seconds. (You can change the valid range and default setting in the <i>Server.properties</i> file. For more information, see Changing MWTM Server Poller Settings, page 3-2 .)

Check Box, Radio Button, or Field	Description
CiscoWorks tab¹	
IP Address or DNS Host Name	The IP address or the DNS host name of the CiscoWorks server.
Port	The access port on the CiscoWorks server. The default setting is 1741.
Secure Port	The port number on the CiscoWorks server that is used for secure access, for example, SSL access. The default setting is 443.
Secure Connection	Indicates if the connection to the CiscoWorks server is secure.

1. Changing these settings affects only the MWTM client you are using. All other MWTM clients retain the CiscoWorks settings that were made during installation or the last time you ran the `mwtm cwsetup` command.

Changing Real-Time Poller and Counter Settings

The MWTM provides three pollers for use in the MWTM client GUI and web pages: a fast, a slow, and a status refresh. You use the MWTM to change settings for those pollers, and also to specify how you want to aggregate the visible counter values.

To change the MWTM poller refresh and counter display settings, use one of these methods:

- The *Server.properties* file specifies minimum, maximum, and default settings for the fast, slow, and status refresh pollers. To change those settings, see [Changing MWTM Server Poller Settings, page 3-2](#).
- To change the MWTM poller refresh and counter display settings for the GUI in the MWTM Preferences window, see [Poller Settings, page 5-6](#).
- To change the MWTM poller refresh and counter display settings for the MWTM web pages by using the MWTM Web Preferences web page, see [Link Reports, page 12-17](#).
- To change the MWTM counter display settings for the GUI from any Real-Time Data and Charts window in the GUI, click **Reset Counters** in any of these MWTM windows:
 - Poll Settings dialog box in any network object's MWTM Details window
 - Node Details: MTP3 Errors table
 - Signaling Point Details: GTT MAP Status table
 - Signaling Point Details: GTT Statistics table
 - Signaling Point Details: MLR Details table

The MWTM displays the MWTM Reset Counters dialog box.

The MWTM Reset Counters dialog box contains:

Field or Button	Description
Show Counters Since Reboot	Click to configure the MWTM client to clear all counters in MWTM web pages whenever the node reboots. The default is clicked.
Show Counters Since Last Poll	Click to configure the MWTM client to clear all counters whenever an MWTM web page is polled. The default is unclicked.
Show Counters Since User Reset	Click to configure the MWTM client to clear all MWTM counters whenever the user resets the counters on an MWTM web page. The default setting for this radio button is cleared.

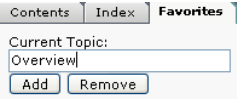
Field or Button	Description
Apply	Applies any changes you made to the counter settings, reflects the changes throughout the MWTM GUI, and closes the MWTM Reset Counters dialog box.
Cancel	Closes the MWTM Reset Counters dialog box.
Help	Displays online help for the current window.

Viewing Online Help

The MWTM client provides links to web-based online help. To display:

Content	In the MWTM client, choose:
Table of contents	Help > Topics
Context-sensitive online help for the current window	Help > Window
MWTM information (build date, version, SSL support, copyright content)	Help > About

The MWTM online help is searchable and supports bookmarking of favorite topics:

Feature	In the MWTM web interface, choose:
Search	
Favorites	

Finding Information in a Window

Sometimes, finding information, such as a node name or event text, in a long list can be difficult. You can use the MWTM client to search for a specific character string in windows that contain lots of information.

**Note**

To find a specific object in the topology window, see [Finding an Object, page 10-16](#).

To find a character string, choose **Edit > Find** from the MWTM main menu. This menu option is available when you select from the navigation tree:

- Active Alarms
- Event History
- Any object under Summary Lists

The MWTM displays the Find dialog box.

**Note**

The Find dialog box also appears when you choose **File > Find** from the Route Table Editor dialog box ([Chapter 13, “Editing an ITP Route Table File”](#)).

The Find dialog box contains:

Field or Button	Description
What	Character string for which the MWTM should search in the window. This can be any character string; all or part of a node name, event text, status, and so on.
Match Case	Check box used to indicate whether the MWTM should search for only character strings that match the case of the text in the What field. To search with: • Case-matching on, select this check box. • Case-matching off, clear this check box. This is the default setting.
Search Forward	Indicates whether the MWTM should search forward (down and to the right) in the window. This radio button is mutually exclusive with the Search Backward button. The default is checked.
Search Backward	Indicates whether the MWTM should search backward (up and to the left) in the window. This radio button is mutually exclusive with the Search Forward button. The default is unchecked.

Field or Button	Description
Find	Launches the search. If: - It finds a matching character string in the window, the MWTM highlights the first line that contains the string. To find the next occurrence of the string, click Find again. You can continue to click Find until you find no more matches in the window. At that time, the MWTM displays an appropriate message in the dialog box, such as: Bottom of table reached. - No matching character string is found, the MWTM displays an appropriate message in the dialog box.
Close	Closes the Find dialog box when you finish searching.

Navigating Table Columns

You can resize, sort, or hide the columns in some tables in the MWTM to meet your specific needs. The MWTM client automatically saves your new settings and, thereafter, launches the client with the new settings.



Note

Hiding table columns is possible in the MWTM client and web interfaces. Resizing table columns is possible only in the client interface. In the web interface, you can search for specific information and page through long tables by using its search and paging features (see [MWTM Web Interface Content Area, page 11-4](#)).

- To view a tooltip for each column in the table, place the cursor over a column heading. If a cell is too small to show all of its text, place the cursor over the cell to see the full text of the tooltip.
- To make a column wider or narrower in the MWTM client interface, click the column divider in the heading and move the divider to the right or left while holding down the left or right mouse button.

All Components or Recent Events tables in the MWTM main window reflect changes that you make to any object's Components or Recent events table. The Show in New window or Real-Time Data and Charts windows do not reflect the changes, however.

Depending on your system, as well as other factors, MWTM windows can sometimes appear so small that text is illegible, and columns and text entry fields too narrow to be usable. If this happens, resize the window and widen the individual columns until the information is again legible and the columns and text entry fields are usable.

- By default, the MWTM displays most of the columns in tables, but some columns may be hidden. To:
 - Display hidden columns, right-click in the table heading and select the check boxes for the columns you want to display. If you are using the web interface, click the **Apply** button.
 - Hide columns, right-click in the table heading and clear the check boxes for the columns you want to hide. If you are using the web interface, click the **Apply** button.

All Components or Recent Events tables in the MWTM main window reflect changes that you make to any object's Components or Recent events table. The Show in New window or Real-Time Data and Charts windows do not reflect the changes, however.

- To sort a table based on the data in a column, left-click in the column heading. The MWTM alpha-numerically sorts the table from top to bottom, based on the data in the chosen column. To sort the table in reverse order, left-click in the column heading a second time. If two entries in the chosen column are identical, the MWTM sorts those rows based on the data in the remaining table columns, moving left to right.
- The tables in the web interface display an icon in the column heading to indicate the column on which the table is sorted, and the direction of the sort. The icon displays a triangle() if the sort order is ascending (1-9, A-Z), and an inverted triangle () if the sort order is descending (Z-A, 9-1).
- If you sort a table in the web interface based on the Nodes column, the MWTM sorts the table based on the DNS names of the nodes, as the MWTM discovers nodes. However, if you modified your preferences to identify nodes by their user-defined names, then the MWTM sorts the table based on the user-defined names of the nodes. For more information, see [Node Name Settings, page 5-5](#).
- To customize the sort order for status settings in the Status column of tables, use the Status settings section of the Preferences window. For more information, see [Changing Status Settings, page 5-12](#).
- (ITP only) To sort a route table, click **Sort Table**. The MWTM sorts the entries in the route table field-by-field, beginning with Dest. Point Code, then Mask, Cost, Dest.Linkset, and finally QoS.

Printing Windows

You can print most MWTM windows, as well as the topology map, for those times when you need hardcopy.

To print an MWTM window, choose **File > Print** from most MWTM windows (for example, the MWTM main window or topology window).

The MWTM displays the Print dialog box.

You use the Print dialog box to specify print settings, such as which printer to print to, whether to send output to a file (the default location for the print file is your home directory), and whether to print duplex.



Note

You can send output to a file only in the file formats that your printer drivers support. Sending output to files can result in large file sizes that you will need to monitor and manage.

When you are satisfied with your print settings, click **Print**. The MWTM prints the window or map.

To exit the Print dialog box at any time without printing, click **Cancel**.

Managing and Deploying ITP Files

You use the MWTM to manage GTT files, route table files, and MLR address table files. The MWTM provides a Node File Management dialog box and a Node Archive Management dialog box:

- [Node File Management, page 5-26](#)
- [Node Archive Management, page 5-33](#)
- [Deploying ITP Files, page 5-36](#)

Node File Management

You use the Node File Management dialog box to:

- View:
 - GTT files
 - Route table files
 - MLR address table files
- Check these files for semantics and syntax
- Delete, rename, and upload the files to a remote node
- Activate the files

The Node File Management dialog box can handle GTT and route table files up to 512 KB in size (the maximum size supported by the MWTM and ITP) and up to 100,000 MLR address table entries.

To launch the Node File Management dialog box, choose **Network > Node File Management** from the MWTM main menu. The MWTM displays the Node File Management dialog box.

**Note**

If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

The Node File Management dialog box contains:

- [Node File Management Menu, page 5-27](#)
- [Node File Management MWTM Pane, page 5-30](#)
- [Node File Management Node Pane, page 5-31](#)

Node File Management Menu

The menu on the Node File Management dialog box contains:

Command	Description
File > Connect (Ctrl-N)	Opens the Pick Node dialog box in which you select a node and connect to that remote node. Note The remote node might be configured to disconnect idle sessions. To prevent disconnection of sessions by the node, enable the MWTM to refresh storage device content automatically by selecting the Enable Auto Refresh Node Storage In Node File Management Dialog check box in the Deploy settings section of the Preferences window, then specify a Refresh Interval. For more information, see Changing Deploy Settings, page 5-16. To avoid entering username and password information each time, you can set up credentials (see Configuring Login Credentials, page 3-20).
File > Disconnect (Ctrl-D)	Disconnects from the node. This option is dimmed if you are not connected to a remote node.
File > Close (Ctrl-W)	Closes the Node File Management dialog box.
Local > Open File	Opens the chosen route table file in the Route Table dialog box (Figure 13-2) or the GTT file in the GTT Editor window (Figure 14-1) or the MLR address table file in the Address Table Editor (Figure 15-1).
Local > Check File	Checks the semantics and syntax of the chosen file on the MWTM client.
Local > Cut	Cuts the chosen local file from the MWTM client.
Local > Copy	Copies the chosen local file from the MWTM client.
Local > Paste	Pastes a cut or copied local file into the MWTM client.
Local > Delete	Deletes the chosen file from the MWTM client. Note If you try to delete a file, and you do not have permission to delete the file, the MWTM issues an appropriate error message.
Local > Rename	Renames the chosen file on the MWTM client. You can use any letters, numbers, or characters in the new name that your operating system allows. However, if you include any spaces in the new name, the MWTM converts those spaces to dashes. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i>.
Local > Refresh	Refreshes the list of files in the MWTM pane. If you have added or modified route table files, GTT files, or MLR files on the MWTM client since you launched the Node File Management dialog box, the MWTM pane reflects those changes.

Command	Description
Local > Go Up	Displays the subdirectories and files that are in the directory that is up one level from the currently visible directory on the MWTM client. This option is dimmed if this is the highest directory level.
Local > Create Directory	Creates a new subdirectory in the directory that the MWTM client currently is displaying.
Remote > Activate	Activates the chosen route table file, GTT file, or MLR file on the remote node. That is, the MWTM replaces the currently running route table file, GTT file, or MLR file on the remote node with the chosen file. Note You cannot activate the <i>MWTM-LAST-ACTIVE-filename.rou</i>, <i>MWTM-LAST-ACTIVE_filename.gtt</i>, <i>MWTM-LAST-ACTIVE-filename.mlr</i>, or <i>MWTM-LAST-ACTIVE-filename.sms</i> files. These are backup files. If you need to revert to one of these files, copy it, rename it, and upload and activate the renamed file on the remote node. This option is dimmed if you are not connected to a remote node.
Remote > Cut	Cuts the chosen remote file from the remote node.
Remote > Copy	Copies the chosen remote file from the remote node.
Remote > Paste	Pastes a cut or copied remote file into the remote node.
Remote > Delete	Deletes the chosen file from the remote node. If you try to delete a file, and you do not have permission to delete the file, the MWTM issues an appropriate error message. Some Cisco routers support redundancy, which requires synchronization of the active and all standby storage devices. If you delete a file in the node pane from an active storage device, and you then try to undelete the file before the standby storage devices have been synchronized, the file will have different IDs on the active and standby storage devices. If this occurs, the MWTM issues this error message and cancels the undelete: Invalid ID You must then undelete the file on the standby storage devices. This synchronization problem does not occur in the MWTM pane. This option is dimmed if you are not connected to a remote node.
Remote > Rename	Renames the chosen file on the remote node. Note You can rename files on the remote node for only Class C devices on the disk drives. You can use any letters, numbers, or characters in the new name that your operating system allows. However, if you include any spaces in the new name, the MWTM converts those spaces to dashes. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i>. This option is dimmed if you are not connected to a remote node.

Command	Description
Remote > Undelete	Recovers the chosen file on the remote node. This option is dimmed if you are not connected to a remote node.
Remote > Refresh	Refreshes the list of files in the node pane. If route table files, GTT files, or MLR files have been added or modified on the remote node since you launched the Node File Management dialog box, those changes appear in the node pane. This option is dimmed if you are not connected to a remote node.
Remote > Go Up	Displays the subdirectories and files that are in the directory that is up one level from the directory that is currently visible on the remote node. This option is dimmed if this is the highest directory level or if you are not connected to a remote node.
Remote > Create Directory	Creates a new subdirectory in the directory that the remote node currently is displaying. Note You can create folders on the remote node for only Class C devices on the disk drives. This option is dimmed if you are not connected to a remote node.
Remote > Squeeze Node	Optimizes Flash memory on the remote node so that the space used by the files marked as <i>deleted</i> or <i>error</i> can be reclaimed. For more information, see the description of the squeeze command in the Cisco IOS Release 12.2 <i>Configuration Fundamentals Command Reference</i> . Note After performing the squeeze process you cannot recover deleted files using Undelete. This option is dimmed if you are not connected to a remote node.
Remote > Format Node	Formats the Flash memory file system on the remote node. For more information, see the description of the format command in the Cisco IOS Release 12.2 <i>Configuration Fundamentals Command Reference</i> . This option is dimmed if you are not connected to a remote node.
Help > Topics (F1)	Displays the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Displays online help for the current window.
Help > About (F3)	Displays build date, version, SSL support, and copyright information about the MWTM application.

Node File Management MWTM Pane

The MWTM pane on the left side of the Node File Management dialog box displays all of the files that the MWTM currently defines on the MWTM client. To populate the MWTM pane with all of the:

- Route table files currently defined on the MWTM client, select **Route Tables** from the drop-down list box.
- GTT files currently defined on the MWTM client, select **GTT Files** from the drop-down list box.
- MLR address table files currently defined on the MWTM client, select **MLR Address Tables** from the drop-down list box.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM sorts this table by Name, and displays all of the columns in the MWTM pane.

See [Navigating Table Columns, page 5-24](#) for more information about resizing, sorting, displaying, or hiding columns.

The MWTM pane contains:

Column	Description
Type	Indicates whether the chosen name is a directory or a file.
Name	Name of the route table, GTT, or MLR file.
Size	Size of the file in bytes.
Modified	Date and time the file was last modified.

The MWTM pane provides these right-click menu options for files:

Command	Description
Open File	Opens the chosen route table file in the Route Table dialog box (Figure 13-2) or the chosen GTT file in the GTT Editor window (Figure 14-1) or the chosen MLR address table file in the Address Table Editor window (Figure 15-1).
Check File	Checks the semantics and syntax of the chosen file on the MWTM client.
Cut	Cuts the chosen file from the MWTM client.
Copy	Copies the chosen file from the MWTM client.
Paste	Pastes a cut or copied file into the MWTM client.
Delete	Deletes the chosen file from the MWTM client. Note If you try to delete a file, and you do not have permission to delete the file, the MWTM issues an appropriate error message.
Rename	Renames the chosen file on the MWTM client. You can use any letters, numbers, or characters in the new name that your operating system allows. However, if you include any spaces in the new name, the MWTM converts those spaces to dashes. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i> .

Command	Description
Refresh	Refreshes the list of files in the MWTM pane. If you have added or modified route table, GTT, or MLR files on the MWTM client since you launched the Node File Management dialog box, the MWTM pane reflects those changes.
Go Up	Displays the subdirectories and files that are in the directory that is up one level from the currently visible directory on the MWTM client. This option is dimmed if this is the highest directory level.
Create Directory	Creates a new subdirectory in the currently visible directory on the MWTM client.
Upload	Uploads the chosen file from the MWTM client to the remote node. You can also upload a file by selecting it in the MWTM pane and clicking the arrow pointing to the node pane. This option, and the arrow, is dimmed if you are not connected to a remote node.

Node File Management Node Pane

The node pane on the right side of the Node File Management dialog box displays all of the files that the MWTM currently defines on the remote node. To populate the node pane with all of the:

- Route table files currently defined on the remote node, select **Route Tables** from the drop-down list box.
- GTT files currently defined on the remote node, select **GTT Files** from the drop-down list box.
- MLR address table files currently defined on the remote node, select **MLR Address Tables** from the drop-down list box.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM sorts this table by Name, and displays all of the columns in the node pane.

See [Navigating Table Columns, page 5-24](#) for more information about resizing, sorting, displaying, or hiding columns.

The node pane contains:

Column	Description
Type	Indicates whether the chosen name is a directory or a file.
Name	Name of the route table, GTT, or MLR file.
Size	Size of the file in bytes.
Modified	Date and time the file was last modified.

The node pane provides these right-click menu options for files:

Right-click Option	Description
Activate	Activates the chosen route table file, GTT file, or MLR file on the remote node. That is, the MWTM replaces the currently running route table file, GTT file, or MLR file on the remote node with the chosen file. Note You cannot activate the <i>MWTM-LAST-ACTIVE-filename.rou</i>, <i>MWTM-LAST-ACTIVE_filename.gtt</i>, <i>MWTM-LAST-ACTIVE-filename.mlr</i>, or <i>MWTM-LAST-ACTIVE-filename.sms</i> files. These are backup files. If you need to revert to one of these files, copy it, rename it, and upload and activate the renamed file on the remote node. This option is dimmed if you are not connected to a remote node.
Cut	Cuts the chosen file from the remote node.
Copy	Copies the chosen file from the remote node.
Paste	Pastes a cut or copied file into the remote node.
Delete	Deletes the chosen file from the remote node. If you try to delete a file, and you do not have permission to delete the file, the MWTM issues an appropriate error message. Some Cisco routers support redundancy, which requires synchronization of the active and all standby storage devices. If you delete a file in the node pane from an active storage device, and you then try to undelete the file before the standby storage devices have been synchronized, the file will have different IDs on the active and standby storage devices. If this occurs, the MWTM issues the following error message and cancels the undelete: Invalid ID You must then undelete the file on the standby storage devices. This synchronization problem does not occur in the MWTM pane.
Rename	Renames the chosen file on the remote node. Note You can rename files on the remote node for only Class C devices on the disk drives. You can use any letters, numbers, or characters in the new name that your operating system allows. However, if you include any spaces in the new name, the MWTM converts those spaces to dashes. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i>.
Undelete	Recovers the chosen file on the remote node.
Refresh	Refreshes the list of files in the node pane. If route table files, GTT files, or MLR files have been added or modified on the remote node since you launched the Node File Management dialog box, those changes appear in the node pane. This option is dimmed if you are not connected to a remote ITP.

Go Up	Displays the subdirectories and files that are in the directory that is up one level from the currently visible directory on the remote node. This option is dimmed if this is the highest directory level.
Create Directory	Creates a new subdirectory in the currently visible directory on the remote node. Note You can create folders on the remote node for only Class C devices on the disk drives.
Squeeze Node	Optimizes Flash memory on the remote node so that the space used by the files marked as <i>deleted</i> or <i>error</i> can be reclaimed. For more information, see the description of the squeeze command in the Cisco IOS Release 12.2 <i>Configuration Fundamentals Command Reference</i> . Note After performing the squeeze process you cannot recover deleted files using Undelete.
Format Node	Formats the Flash memory file system on the remote node. For more information, see the description of the format command in the Cisco IOS Release 12.2 <i>Configuration Fundamentals Command Reference</i> .
Download	Downloads the chosen file from the remote node to the MWTM client. You can also download a file by selecting it in the node pane and clicking the arrow pointing to the MWTM pane.

Node Archive Management

You use the Archive Management dialog box to view the contents of the archive, open a version with its corresponding editor, and delete all versions of a file.

To launch the Archive Management dialog box, choose **Edit > Node Archive Management** from the MWTM main menu. The MWTM displays the Archive Management dialog box.



Note

If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

The Archive Management dialog box contains:

- [Node Archive Management Menu, page 5-34](#)
- [Node Archive Management Selector Pane, page 5-34](#)
- [Node Archive Management Display Pane, page 5-35](#)

Node Archive Management Menu

The menu on the Archive Management dialog box contains:

Command	Description
File > Open File	Opens the chosen route table file in the Route Table dialog box (Figure 13-2) or the chosen GTT file in the GTT Editor window (Figure 14-1) or the chosen MLR address table file in the Address Table Editor window (Figure 15-1).
File > Delete	Deletes all versions of the chosen file from the MWTM client. Note If you try to delete a file, and you do not have permission to delete the file, the MWTM issues an appropriate error message.
File > Refresh	Updates data for the currently visible entries.
File > Close (Ctrl-W)	Closes the Archive Management dialog box.
Help > Topics (F1)	Displays the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Displays online help for the current window.
Help > About (F3)	Displays build date, version, SSL support, and copyright information about the MWTM application.

Node Archive Management Selector Pane

The selector pane on the left side of the Archive Management dialog box displays all of the files that the MWTM currently defines on the MWTM client. To populate the selector pane with all of the:

- Route table files currently defined on the MWTM client, select **Route Tables** from the drop-down list box.
- GTT files currently defined on the MWTM client, select **GTT Files** from the drop-down list box.
- MLR address table files currently defined on the MWTM client, select **MLR Address Tables** from the drop-down list box.

To see the tooltip for each button in the selector pane, place the cursor over the button.

The selector pane contains:

Button or Object	Description
Open File	Opens the chosen route table file in the Route Table dialog box (Figure 13-2) or the chosen GTT file in the GTT Editor window (Figure 14-1) or the chosen MLR address table file in the Address Table Editor window (Figure 15-1).
Delete	Deletes all versions of the chosen file from the MWTM client. Note If you try to delete a file, and you do not have permission to delete the file, the MWTM issues an appropriate error message.
Refresh	Updates data for the currently visible files.
Nodes	To see the nodes, signaling points, and archived files associated with a specific node, click the turner  beside the node or signaling point. Clicking on an archived file displays the file in the right pane.
Signaling Points	To see the signaling points and archived files associated with a specific signaling point, click the turner  beside the signaling point. Clicking on an archived file displays the file in the right pane.

The selector pane provides these right-click menu options for files:

Command	Description
Open File	Opens the chosen route table file in the Route Table dialog box (Figure 13-2) or the chosen GTT file in the GTT Editor window (Figure 14-1) or the chosen MLR address table file in the Address Table Editor window (Figure 15-1).
Delete	Deletes all versions of the chosen file from the MWTM client. Note If you try to delete a file, and you do not have permission to delete the file, the MWTM issues an appropriate error message.

Node Archive Management Display Pane

The Archive Management pane displays all of the versions that currently exist on the chosen file in a table. To navigate to a chosen file, click the turner  beside Nodes or Signaling Points in the selector pane (in the left pane), and click on the file. All versions appear in the right pane.

If a cell is too small to show all of its comments, place the cursor over the cell to see the full text in a tooltip.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM sorts this table by Rev and displays all of the columns in the display pane.

See [Navigating Table Columns, page 5-24](#) for more information about resizing, sorting, displaying, or hiding columns.

The display pane contains:

Column or Button	Description
Rev	Revision number.
Date	Date of archival.

Column or Button	Description
Comments	Archival comments.
Author	User or client hostname or IP address from which the deployment or archiving occurred.
Adjust row height	You can adjust the row height to make comments readable.

The display pane provides this right-click menu option for files:

Command	Description
Open File	Opens the chosen route table file in the Route Table dialog box (Figure 13-2) or the chosen GTT file in the GTT Editor window (Figure 14-1) or the chosen MLR address table file in the Address Table Editor window (Figure 15-1).

Deploying ITP Files



Tip

Before you can use the Deployment Wizard, you must set up TFTP (for details, see [Setting Up TFTP on Your Server \(ITP Only\)](#), page 3-12).

You use the Deployment Wizard to validate a route table file, GTT file, or MLR address table file, upload it to an ITP, archive the file, and activate it on the ITP. The Deployment Wizard can handle route table and GTT files up to 512 KB in size (the maximum size the MWTM and ITP support) and up to 100,000 MLR address table entries.

To launch the Deployment Wizard, choose **File > Deploy** from the route table menu, GTT menu, or Address Table Editor menu. The MWTM displays the Deployment Wizard for the currently visible file.

Figure 5-2 Deployment Wizard for a GTT File

** Illustration to be supplied **

The left pane of the Deployment Wizard contains:

Step	Description
Select File	Indicates that the file is chosen for deployment. The name of the file to deploy appears in the Deployment Wizard title bar.
Select Node/SP	If you are deploying a GTT file or address table file, you use this option to select the signaling point to deploy the file. You can optionally check the Filter by Node check box, which limits signaling point selection to a specific node. Select a signaling point and node (optional) from the drop-down list boxes in the right pane, then click Next >. If you are deploying a route table file, the MWTM proceeds directly to the Validate step.
Validate	Validates the file for deployment. Validation messages and error messages, if any, appear in the right pane.

Step	Description
Login	You can log in to the signaling point. If required, enter the: • Login username, if required. • Login password, if required. • Enable username, if required. • Enable password, if required. Note To avoid entering username and password information each time, you can set up credentials (see Configuring Login Credentials, page 3-20).
Upload	Uploads the file to the signaling point. If the file uploads with no errors, the MWTM proceeds to the Activate step. If the specified file already exists on the ITP, the MWTM displays the name of the duplicate file and the Overwrite and Always Overwrite check boxes. Check the: • Overwrite check box to overwrite the file on the ITP with the file being deployed. This is the default setting. • Always Overwrite check box if you want the MWTM to always overwrite the file on the ITP with the file being deployed, without prompting you for confirmation. The default setting for this check box is unchecked (prompt for confirmation). If you have set your preferences so that the MWTM client identifies nodes by their DNS names (the default setting) instead of by their IP addresses, then the ITP must be able to resolve the DNS names. Otherwise, the MWTM issues an appropriate error message and does not deploy the file. To enable the ITP to resolve DNS names, enter the ip domain-lookup command on the ITP. For more information about this command, see the <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i>, Release 12.3 or later. For more information about the Show DNS or User-Defined Names and Show IP Address in Name Field preference settings, see Node Name Settings, page 5-5.
Archive	You use to enter archive comments, if required. If archive comments are not required, the MWTM displays the Always Skip Archive Comments check box. For details on setting archive comments to required or optional, see mwtm deployarchive, page B-94.
Activate	Activates the file on the signaling point (replaces the currently running route table file, GTT file, or address table file with the deployed file). The MWTM displays the Activate File and Always Activate File check boxes. You can: • Check the Activate File check box to activate the deployed file on the ITP. This is the default setting. • Uncheck the Activate File check box if you do not want to activate the deployed file on the ITP yet. • Check the Always Activate File check box if you want the MWTM to always activate the deployed file on the ITP, without prompting you for confirmation. The default setting for this check box is cleared (prompt for confirmation).
Done	Displays any status messages, such as errors or successful completion.

The bottom line of the Deployment Wizard contains:

Field or Button	Description
Progress Bar	Indicates that the MWTM is validating or uploading the file.
Show Log/Hide Log	Displays or hides the log file for the Deployment Wizard.
Next >	Advances to the next step in the Deployment Wizard.
Finish	Closes the Deployment Wizard. The Finish button appears when deployment ends successfully, or when the MWTM encounters errors and cancels the process.
Cancel	Closes the Deployment Wizard without deploying the file.
Help	Displays online help for the Deployment Wizard.

Exporting Data

You use the MWTM to export its data for use by other products, such as CiscoWorks or Microsoft Excel. This section includes:

- [Exporting Current Data for Network Objects, page 5-38](#)
- [Exporting Current Node Names and SNMP Community Names, page 5-39](#)

Exporting Current Data for Network Objects

You can use the MWTM CLI to export all MWTM data, or to export only chosen MWTM data.

To export all current MWTM data, with fields separated by vertical bars (|; this is the default setting), enter the **mwtm export all** command with the **-d bar** keywords:

mwtm export all -d bar

To export all MWTM data with fields separated by commas (,), specify the **-d comma** keywords:

mwtm export all -d comma

To export all MWTM data with fields separated by tabs, specify the **-d tab** keywords:

mwtm export all -d tab

To export only object-specific MWTM data, specify one of these keywords:

- **as**—(ITP only) Export only application server data.
- **asp**—(ITP only) Export only application server process data.
- **aspa**—(ITP only) Export only application server process association data.
- **links**—(ITP only) Export only link data.
- **linksets**—(ITP only) Export only linkset data.
- **nodes**—Export only node data.
- **sgmp**—(ITP only) Export only signaling gateway-mated pair data.
- **sps**—(ITP only) Export only signaling point data.

You can also specify the **-d comma** or **-d tab** keywords on any of these object-specific **mwtm export** commands.

Here is sample output for the **mwtm export nodes** command:

```
# ./mwtm export nodes
# v6.1.0.15
# t1168093931311|Sat Jan 06 09:32:11 EST 2007
#
# Total 2 nodes
# name|displayname|sgmid|old_description|cllicode|ipaddress|old_pointcode|old_se
condary|old_capability|state|statetimestamp|ioslevel|devicetype|usericonname|sys
descr|lastpolltimestamp|lastpolltime|avgpolltime|old_lasterrormsg|old_lasterrort
ime|notesexist|old_variant|sysuptime|rebootreason|statereason|discoveredtime|eve
ntRcvd|connectTo|ignore|customName|processTraps|nsoconfig|mtp3offload|rfpeerstat
e|trapPollingEnabled|reportPollingEnabled|sysName|nodeType

ems1941ka.cisco.com|ems1941ka.cisco.com|1253|not_used|not_used|[172.18.156.20][2
0.1.1.105]|not_used|not_used|not_used|Warning|1168092733287|7|CiscoMWR-1941-DC|n
ull|sysDescr|1168093830179|328|634|not_used|not_used|false|not_used|248128063|re
load|62|1168092732082|false|null|false|null|true|not_used|not_used|not_used|true
|true|ems1941ka|RAN-O

sgm-26-91c-2.cisco.com|null|1350|not_used|clli_2691c|[172.18.17.132,172.18.17.4]
[]|not_used|not_used|not_used|Unmanaged|1168093760605|31|Cisco2651XM|null|sysDes
cr|1168092856198|12984|18729|not_used|not_used|false|not_used|731561022|reload|1
|1168092734928|false|null|false|null|true|1|1|2|false|false|sgm-26-91c.cisco.com
|ITP
```

For more information about the use of the **mwtm export** command, see [mwtm export](#), page B-30.

Exporting Current Node Names and SNMP Community Names

To export current MWTM node names and read and write SNMP community names, in CiscoWorks import format, with fields separated by commas (,), specify the **cw** keyword:

mwtm export cw

You can export this data to a file, then use the file to import the nodes into the CiscoWorks database.

For more information about the use of the **mwtm export cw** command, see [mwtm export cw](#), page B-31.

Integrating the MWTM with Other Products

The MWTM does not require CiscoWorks or the Cisco Info Center (CIC), but the MWTM does integrate with those products to provide added value. See these sections for more information:

- [Integrating the MWTM with CiscoWorks](#), page 5-39
- [Forwarding Traps to Other Hosts \(Server Only\)](#), page 5-42

Integrating the MWTM with CiscoWorks

The MWTM can integrate with CiscoWorks during installation, registering with CiscoWorks as an installed application. In this scenario, CiscoWorks and MWTM are running on the same server. See the “Installing the MWTM on Solaris” and “Installing the MWTM on Windows” chapters of the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for more information.

You can also integrate the MWTM with CiscoWorks after installation by using:

- Preference settings. See [Changing CiscoWorks Server Settings, page 5-13](#).
- The **mwtm cwsetup** command. See [mwtm cwsetup, page B-21](#), for more information.

Once you have integrated the MWTM with CiscoWorks, you can:

- [Launch CiscoWorks Applications from the MWTM Client, page 5-40](#)
- [Launch Integrated Applications from the MWTM Web Interface, page 5-41](#)
- [Launch the MWTM Web Interface from the CiscoWorks Dashboard, page 5-42](#)

Launch CiscoWorks Applications from the MWTM Client

When you integrate the MWTM with CiscoWorks, you can launch, from the MWTM client Tools > Launch menu, the:

- CiscoView
- CiscoWorks LMS Portal
- Content Services Gateway (CSG) Service Manager
- CiscoWorks Device Center
- GPRS Gateway Support Node (GGSN) Service Manager

To launch CiscoWorks applications from the MWTM client:

Step 1 Ensure that CiscoWorks is installed in the network.

Step 2 To launch the appropriate CiscoWorks application:

CiscoWorks Application	Description	Steps to Launch from MWTM
CiscoView	Provides a real-time, color-coded, graphical representation of Cisco devices. You can use CiscoView to quickly identify an incorrect status on a port or interface. If you are running CiscoWorks on UNIX or Windows, you can access CiscoView through the link to the web version of CiscoWorks.	Choose Tools > Launch > CiscoView from the MWTM main menu. Or, right-click a node in the navigation tree and choose Launch > CiscoView .
CiscoWorks LMS Portal	Provides a dashboard of CiscoWorks tools and utilities such as Resource Manager Essentials.	Choose Tools > Launch > CiscoWorks LMS Portal from the MWTM main menu.
CSG Service Manager	Provides a wizard-based workflow to provision CSG1 and CSG2 features in the network.	Choose Tools > Launch > CSG Service Manager from the MWTM main menu. ¹

CiscoWorks Application	Description	Steps to Launch from MWTM
Device Center	Provides useful web-based device-monitoring functions, including reachability trends, response time trends, interface status, Syslog browsing, and a detailed inventory.	Choose Tools > Launch > Device Center from the MWTM main menu. Or, right-click a node in the navigation tree and choose Launch > Device Center .
GGSN Service Manager	Provides a wizard-based workflow to provision GGSN devices.	Choose Tools > Launch > GGSN Service Manager from the MWTM main menu. ¹

1. The MWTM attempts to launch the URL of the service manager that resides on the LMS server. If the service manager is not installed on the LMS server, you will receive an HTTP 404 error. To prevent this error, ensure that the service managers are installed on the LMS server, or remove the CSG or GGSN network setting with the **mwtm manage** command.

Step 3 At the prompt, enter a CiscoWorks user ID and password.

Depending on your selection in [Step 2](#), the MWTM links to the:

- Device Center dashboard, which displays information about the chosen node.
- CiscoView, which shows a graphical representation of the chosen node.
- CSG Service Manager
- GGSN Service Manager

Launch Integrated Applications from the MWTM Web Interface

To launch integrated applications from the MWTM web interface:

Step 1 From the MWTM web interface, click the **Tools** link in the navigation tree (left pane).



Note If CiscoWorks does not appear in the navigation tree of the MWTM web interface, CiscoWorks is not integrated with the MWTM. Use the [mwtm cwsetup](#), [page B-21](#), to integrate CiscoWorks with the MWTM.

Step 2 In the right pane, in the Launch pane, click:

- CiscoView (*server_name*)
- CiscoWorks LMS Portal (*server_name*)
- CSG Service Manager (*server_name*)
- Device Center (*server_name*)
- GGSN Service Manager (*server_name*)

The chosen application launches.

**Note**

The MWTM attempts to launch the URL of the service manager that resides on the LMS server. If the service manager is not installed on the LMS server, you will receive an HTTP 404 error. To prevent this error, ensure that the service managers are installed on the LMS server, or remove the CSG or GGSN network setting with the **mwtm manage** command.

Launch the MWTM Web Interface from the CiscoWorks Dashboard

To launch the MWTM web interface from the CiscoWorks dashboard:

Step 1 Log in to your CiscoWorks dashboard.

Step 2 In the Mobile Wireless Transport Manager box, click the **MWTM Server Home Page** link.

**Note**

If the Mobile Wireless Transport Manager box does not appear, CiscoWorks is not integrated with the MWTM. Use the [mwtm cwsetup](#), page B-21, to integrate CiscoWorks with the MWTM.

The MWTM web interface opens to the home page.

Forwarding Traps to Other Hosts (Server Only)

You use the MWTM to forward SNMP traps to other SNMP servers, or hosts. The MWTM can then function as a trap multiplexer, integrating with high-level event- and alarm-monitoring systems such as the Cisco Info Center and Micromuse's Netcool suite of products. These systems can provide a single high-level view of all alarm monitoring in your network, making it easier to detect and resolve problems.

To enable the MWTM to forward SNMP traps to other hosts, specify the list of hosts in the *TrapForwarder.properties* file. The default file resides in the MWTM */properties* directory. If you installed the MWTM in:

- The default directory, */opt*, then the default file resides in */opt/CSCOsgm/properties/TrapForwarder.properties*.
- A different directory, then the default file resides in that directory.

In the *TrapForwarder.properties* file, begin all comment lines with a pound sign (#).

All other lines in the file are host definition lines using this format:

```
SERVERxx=dest-address[:portno]
```

where:

- *xx* is the user-defined server number.
- *dest-address* is the hostname, or the IP address in dotted-decimal format.
- *portno* is the optional port number. The default port number is 162.

For example, this host definition line:

SERVER02=64.102.86.104:162

enables the MWTM to forward traps to Server 02, with IP address 64.102.86.104, on port 162.

Any changes you make to the *TrapForwarder.properties* file take effect when you restart the MWTM server. Thereafter, the MWTM forwards all traps from the listed hosts except traps:

- That the MWTM cannot parse.
- From hosts listed in the *trapaccess.conf* file. For more information, see [Limiting Traps by IP Address, page 3-9](#).

The MWTM modifies Version 2c traps that do not have the agent IP address already specified in the varbind list by including the agent IP address in the varbind list.

You can also forward MWTM events to other hosts, in the form of SNMP traps. For more information, see [Forwarding Events as Traps to Other Hosts, page 9-48](#).

Running Simultaneous Client Sessions

You can run multiple sessions of the MWTM client simultaneously because the MWTM uses a client-server architecture. The MWTM server provides central services and database functions and communicates with multiple MWTM clients. You can install the MWTM client software on the same system as the MWTM server, or on a different system on the same network as the MWTM server.



Note

Running more than one MWTM client on the same workstation can degrade the workstation performance.

The MWTM recommends a maximum of 20 clients per MWTM server. If you connect more than 20 clients to a single server, the server requires additional memory and a more powerful CPU.

Performing Basic Server Operations

This section contains this information:

- [Connecting to a New Server, page 5-43](#)
- [Viewing Server Status Information, page 5-44](#)

Connecting to a New Server

You use the MWTM to connect the client to a new MWTM server. For example, you can monitor two or more networks from the same MWTM client, simply by switching servers. Or, if you have two MWTM servers monitoring the same network, and one server fails, the MWTM client automatically switches to the secondary server.

If you want to determine the default hostname before you connect to the new server, it appears in the SERVER_NAME entry in the *System.properties* file. If you installed the MWTM in:

- The MWTM in the default directory, */opt*, then the location of the *System.properties* file is */opt/CSCOs/gm/properties/System.properties*.
- A different directory, then the *System.properties* file resides in that directory.

To connect the client to a new server, choose **File > Connect to New Server** from the MWTM main menu. The MWTM displays the Connect to New Server dialog box.

The Connect to New Server dialog box contains:

Field or Button	Description
Server Name or IP Address	Name or IP address of the new server. Enter the name of the new server, or its IP address, in the Server Name or IP Address field.
Name Server Port	UDP port number for the new server. Enter the MWTM Naming Server UDP port number for the new server in the Name Server Port field. The default value is 44742.
OK	Stops the MWTM client, then restarts the client connected to the specified server. When you have entered the name of the new server, or its IP address, and its UDP port number, click OK . The MWTM stops the client, then restarts the client connected to the new server.
Cancel	Closes the Connect to New Server dialog box without connecting to the new server.
Help	Displays online help for the Connect to New Server dialog box.

Viewing Server Status Information

You use the MWTM to view detailed information about the processes, pollers, tasks, and clients for the server to which you are connected.

To display server status information, choose **View > MWTM Server > Status** in the MWTM main menu. The MWTM displays the Server Status Information window.

Figure 5-3 **Server Status Information Window**

** Illustration to be supplied **

The Server Status Information window contains:

- [Server Status Information: Fields and Buttons, page 5-44](#)
- [Server Status Information: Processes, page 5-45](#)
- [Server Status Information: Pollers, page 5-45](#)
- [Server Status Information: Tasks, page 5-46](#)
- [Server Status Information: Clients, page 5-46](#)

Server Status Information: Fields and Buttons

The Server Status Information window contains:

Command	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays a message that the MWTM is polling the device. After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Update	Forces an immediate poll, and refreshes the Server Status Information window with the latest data.
Close	Closes the Server Status Information window.
Help	Accesses the online help for this window.

Server Status Information: Processes

The Server Status Information: Processes section lists the processes that make up the MWTM server, and contains:

Field	Description
Name	Name of the process, such as sgmNameServer.
Process ID	Number to uniquely identify the process.
Is Running	Indicates whether the process is running (true) or not (false).

Server Status Information:Pollers

The Server Status Information: Pollers table lists the detail and demand pollers that the MWTM server is currently processing, and contains:

Field	Description
Poller ID	Number to uniquely identify each MWTM detail poller that is currently active. MWTM detail pollers collect detailed data (such as real-time data, statistics, route detail, and so on) that the regular MWTM poller did not collect.
Client Host	Name of the MWTM client that started the detail poller.
Interval	Poll interval for the detail poller, in hours, minutes, and seconds.
Iteration	Number of times the detail poller should poll. If this field displays Forever, the detail poller will never stop polling, until the MWTM client requests that it stops.
Next Poll	Time until the next poll, in hours, minutes, and seconds.
Time Limit	Time remaining, in hours, minutes, and seconds, until the poller times out. When the poller times out, the MWTM automatically stops the poller to prevent unnecessary traffic on the network and sends an appropriate error message to the client. By default, the MWTM allows pollers to run up to 8 hours. To change that setting, see the description of the mwtm pollertimeout command in mwtm pollertimeout , page B-49.
Description	Description of the detail poller.

Server Status Information:Tasks

The Server Status Information: Tasks table lists long-running services that the MWTM server performs, and contains:

Field	Description
Task ID	Number to uniquely identify the task.
Interval	Time between runs for the task, in hours, minutes, and seconds.
Iteration	Number of times the task should run. If this field displays Forever, the task will never stop polling.
Next Execution	Time until the next run for the task, in hours, minutes, and seconds.
State	Current state of the task. Valid values are: • None—Task is stopped. • Waiting—Task is waiting to transition to Ready or Running state. • Ready—Task is ready to execute but is not yet in Running state. • Running—Task is started and is currently executing. • Pending—Task was in Ready state when a user canceled it. The task is pending final removal from the scheduler. • Error—Task encountered an error. • Dying—Task was in Running state when it was canceled by a user. The task continues to run in Dying state until it ends. The server then removes the task from the scheduler.
Description	Description of the task.

Server Status Information: Clients

The Server Status Information: Clients table contains:

Field	Description
Process Name	Name of an MWTM client that is currently connected to the server.
User Name	If you have implemented MWTM User-Based Access, this field displays the name of an MWTM client user who is currently logged in and connected to the server. If you have not implemented MWTM User-Based Access, this field displays the name of the node that the user is using.
Message Mask	Mask that indicates which messages can be sent to the client.
Sleeping?	Indicates whether the thread that is responsible for delivering messages is sleeping (yes) or not (no). The normal setting for this field is no.
Sleep Time	Time in seconds the thread that is responsible for delivering messages has been sleeping. The normal setting for this field is 0.
Queue Size	Number of messages waiting to be sent to the MWTM client. The normal setting for this field is 0, but it could be higher if the MWTM server or client is very busy, as during Discovery.

Using the Command Line Interface

The MWTM provides a command line interface that you use to interact with the MWTM and with the Cisco IOS software operating system by entering commands and optional arguments. For more information, see [Appendix B, “Command Reference.”](#)



CHAPTER 6

Understanding Basic Object Functions

You can use the Cisco Mobile Wireless Transport Manager (MWTM) to view basic information about any discovered MWTM object, including its associated objects, status, and other important information.

To view basic information for an object, click the turner beside Summary Lists in the navigation tree of the MWTM main window, then select one of these objects:



Note

Objects only appear if your network contains that particular object type.

Object	Applicable Network Type
Alarms	All networks
Nodes	All networks
Signaling Points	ITP only
Note In a multi-instance network, the signaling point name has the format <i>pointcode:instanceName</i> . In a multi-instance network, the MWTM does not display signaling points that are only partly configured (that is, the variant and network name are configured, but not the primary point code).	
Linksets	
Links	
Application Servers	
Application Server Processes	
Application Server Process Associations	
Signaling Gateway Mated Pairs	
Interfaces	All networks

Object	Applicable Network Type
Cards	RAN-O only
RAN Backhauls	
RAN Shorthauls	
Access Point Names	mSEF only

This chapter contains:

- [Displaying Object Windows, page 6-2](#)
- [Editing Properties, page 6-33](#)
- [Attaching Notes, page 6-38](#)
- [Viewing Notes, page 6-39](#)
- [Deleting Objects, page 6-40](#)
- [Unmanaging and Managing Nodes or ITP Signaling Points, page 6-42](#)
- [Excluding Nodes or ITP Signaling Points from a View, page 6-43](#)
- [Ignoring and Unignoring Objects, page 6-43](#)

Displaying Object Windows

To display an object window, in the MWTM main window, under Summary Lists in the navigation tree, click the object type. The object window appears in the right pane.

Example:

To display the nodes table, choose **Summary Lists > Nodes**. The nodes table appears.

- The table lists all objects of the object type that you chose in the navigation tree. To see the fully qualified domain name (FQDN) of any object in the table, hover over the object with the mouse. A tooltip lists the FQDN for the object.
- Some table columns may be hidden by default. To see a list all columns, right-click on any column, and check the box for the columns that you want to expose.
- Tables are sorted based on the column that is highlighted. To sort by a different column, simply click the desired column.



Tip

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

Figure 6-1 Node Window

Name	Primary SNMP Address	Node Type	Feature	Software Version	Ignored	Trap Polling	Report Polling	Notes	Events	Severity	Status	Status Reason
ems7613c	172.18.175.37	Cisco7613	Unkno...	12.2(17...	☐	☒	☐			Major	Active	None
sgm-76-92b-2	172.18.17.176	Cisco7613	ITP	12.2(18)...	☐	☒	☒			Critical	Warning	Link Inactive
sgm-76-94k-2	172.18.17.236	Cisco7604	ITP	12.2(18)...	☐	☒	☒			Major	Warning	Linkset Inactive
sgm-76-92c	172.18.17.34	Cisco7606	ITP	12.2(18)...	☐	☒	☒			Major	Warning	Link Inactive
sgm-76-93a-2	172.18.17.206	Cisco7604	ITP	12.2(18)...	☐	☒	☒			Major	Warning	Linkset Inactive
sgm-76-91a	172.18.17.16	Cisco7604	ITP	12.2(18)...	☐	☒	☒			Normal	Warning	Mate not Active
sgm-73-90i	172.18.16.9	Cisco7301	Unkno...	12.2(18)...	☐	☐	☐			Unmanaged	Unmanaged	None
ems7609osr3	172.18.126.192	cat6509Sp	Unkno...	12.2(18)...	☐	☒	☐			Major	Active	None
ems7604a	172.18.126.140	Cisco7604	Unkno...	12.2(18)...	☐	☒	☐			Normal	Active	None
ems7604c	172.18.126.62	Cisco7604	CSG1	12.2(18)...	☐	☒	☐			Normal	Active	None
ems7609osr...	172.18.126.98	cat6509Sp	CSG1	12.2(18)...	☐	☒	☐			Major	Active	None
ems7613g	172.18.102.199	Cisco7613	CSG1	12.2(18)...	☐	☒	☐			Major	Active	None
sgm-75-90b-2	172.18.16.131	Cisco7507mx	ITP	12.2(19)...	☐	☒	☒			Normal	Warning	Link Inactive
sgm-75-90a-2	172.18.16.130	Cisco7507mx	ITP	12.2(20)...	☐	☒	☒			Normal	Warning	Linkset Inactive
sgm-26-91i	172.18.17.10	Cisco2651XM	ITP	12.2(20)...	☐	☒	☒			Normal	Warning	Link Inactive
sgm-75-94b-2	172.18.17.227	Cisco7507mx	ITP	12.2(20)...	☐	☒	☒			Normal	Warning	Link Remote Int
sgm-75-93a-2	172.18.17.194	Cisco7507	ITP	12.2(20)...	☐	☒	☒			Normal	Warning	Link Inactive
sgm-26-90k-2	172.18.16.151	Cisco2651XM	ITP	12.2(21)...	☐	☒	☒			Normal	Warning	Link Inactive
sgm-26-90l-2	172.18.16.141	Cisco2651XM	ITP	12.2(23)...	☐	☒	☒			Normal	Warning	Link Inactive
sgm-26-93e-2	172.18.17.198	Cisco2651	ITP	12.2(23)...	☐	☒	☒			Normal	Active	None
sgm-26-92b-2	172.18.16.139	Cisco7301	ITP	12.2(25)...	☐	☒	☒			Normal	Warning	SGMP Inactive
sgm-26-93f-2	172.18.17.199	Cisco2651	ITP	12.2(25)...	☐	☒	☒			Normal	Active	None
sgm-75-92b	172.18.17.35	Cisco7507z	ITP	12.2(25)...	☐	☒	☒			Minor	Warning	Mate not Active
sgm-75-91b	172.18.17.3	Cisco7507mx	ITP	12.2(25)...	☐	☒	☒			Normal	Warning	Link Inactive
sgm-75-91a	172.18.17.2	Cisco7507	ITP	12.2(25)...	☐	☒	☒			Normal	Warning	Link Inactive

Object windows provide information about all objects of a specific type that the MWTM has discovered.

Object windows can contain:

- [Right-Click Menu for All Objects, page 6-4](#)
- [Alarms Table, page 6-4](#)
- [Nodes Table, page 6-5](#)
- [Signaling Points Table, page 6-8](#)
- [Linksets Table, page 6-10](#)
- [Links Table, page 6-13](#)
- [Application Servers Table, page 6-14](#)
- [Application Server Processes Table, page 6-16](#)
- [Application Server Process Associations Table, page 6-18](#)
- [Signaling Gateway Mated Pairs Table, page 6-19](#)
- [Interfaces Table, page 6-21](#)
- [Cards Table, page 6-23](#)
- [RAN Backhauls Table, page 6-25](#)
- [RAN Shorthauls Table, page 6-27](#)
- [Access Point Names Table, page 6-29](#)
- [Software Versions Table, page 6-30](#)

Right-Click Menu for All Objects

To see the right-click menu for all objects, in the MWTM main window, under Summary Lists in the navigation tree, select the object type and right-click it. The right-click menu contains:

Menu Command	Description
Show in New Window	Opens the object window in a new window.
Back > List of Windows	Navigates back to a window viewed in this session. The MWTM maintains a list of up to 10 Back windows.
Forward > List of Windows	Navigates forward to a window viewed in this session. The MWTM maintains a list of up to 10 Forward windows.



Note

The right-click menu, available by clicking on a specific object in the right pane, is described in [Viewing the Right-Click Menu for an Object, page 8-3](#).

Alarms Table

The alarms table displays a count of alarms by node and severity. To display the alarms table, choose **Summary Lists > Alarms**. The alarms table contains:

Column	Description
Internal ID (MWTM client only)	Internal ID of the node. The internal ID is a unique ID for every object, which the MWTM assigns for its own internal use. This ID can also be useful when the TAC is debugging problems.
Node	Name of the node.
Total	Total number of alarms for the node.
Critical	Total number of critical alarms for the node.
Major	Total number of major alarms for the node.
Minor	Total number of minor alarms for the node.
Warning	Total number of warning alarms for the node.
Informational	Total number of informational alarms for the node.
Indeterminate	Total number of indeterminate alarms for the node.

Nodes Table

The nodes table displays information about nodes that the MWTM has discovered. To display the nodes table, choose **Summary Lists > Nodes**. The nodes table contains:

Column	Description
Internal ID	Internal ID of the node. The internal ID is a unique ID for every object, which the MWTM assigns for its own internal use. This ID can also be useful when the TAC is debugging problems.
Name	Name of the node.
Primary SNMP Address	IP address of the node, which SNMP uses to poll the node. (There might be other IP addresses on the node that are not the primary SNMP address.)
CLLI Code (ITP only)	Common Language Location Identification code for the node. A CLI code is a standardized 11-character identifier that uniquely identifies the geographic location of the node. If the node has no CLI code configured, this field is blank.
Node Type	Description of the hardware platform that supports a feature. ITP Node Types • Cisco2650XM, Cisco2651XM • Cisco2811 • Cisco7204VXR, Cisco7206VXR • Cisco7301 • Cisco7507, Cisco7507mx, Cisco7507z, Cisco7513, Cisco7513mx, Cisco7513z • Cisco 7603, Cisco 7603s, Cisco7604, Cisco7606, Cisco7606s, Cisco7609, Cisco7609s, Cisco7613

Column	Description
Node Type (continued)	IPRAN Node Types - Cell Site Routers (CSR): - CiscoMWR-1941-DC—Cisco MWR-1941-DC-A series router - Cisco3825—Integrated Services Router - CiscoONS15454—Cisco ONS 15454 SONET multiplexer - RAN_SVC—RAN Service Module in the Cisco ONS 15454 mSEF Node Types - CiscoSAMI—Service Application Module for IP (SAMI) - CiscoMWAM—Multiprocessor WAN Application Module (MWAM) Other Node Types - IPDevice—IP device, other than those listed previously. You can assign this icon to an unknown node if you know that it is an IP device. - Unknown—MWTM is unable to determine the node type. - Linux—Hardware platform for Cisco Database for Telecommunications (CDT)
Feature	Primary function performed by a node type: - ITP—IP Transfer Protocol - IPRAN features: - ONS—Optical Networking Service - RAN_SVC—RAN Service - CSR—Cell Site Router - mSEF features: - CSG1 or CSG2—Content Services Gateway - GGSN—Gateway GPRS Support Node - HA—Home Agent - BWG Gateway—Broadband Wireless Gateway - CDT—Cisco Data for Telecommunications (CDT)
Software Version	Version of node's software.
Serial Number	Serial number of the node.
Uptime	Time the node has been up, in days, hours, minutes, and seconds.
Reboot Reason	Reason for the last reboot of the node.

Column	Description
Ignored	Indicates whether to include the node when aggregating and displaying MWTM status information: • Check the check box to include the node. This is the default setting. • Uncheck the check box to exclude the node. Note Not applicable for unmanaged nodes. Users with authentication level Power User (level 2) and higher can edit this field.
Process Traps	Indicates whether the MWTM should process traps from this node. This field is read-only.
Trap Polling	Indicates whether trap polling is enabled for this node. This field is read-only. • If you want to enable trap polling for this node, set ipran-mib snmp-access to inBand on the node. • If you want to disable trap polling for this node, set ipran-mib snmp-access to outOfBand on the node.
Report Polling	Indicates whether report polling is enabled for this node. This field is read-only. • If you want to enable report polling for this node, set ipran-mib location to aggSite on the node. • If you want to disable report polling for this node, set ipran-mib location to cellSite on the node.
Notes	Indicates whether a note is associated with the node.
Events (MWTM client only)	Indicates whether the node has received any events. If the node has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the node.
Last Status Change	Date and time that the status of the node last changed.
Severity	Indicates the alarm severity for the chosen node. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.

Column	Description
Status	Current status of the node. Possible values are:  Active  Discovering  Polling  Unknown  Unmanaged  Waiting  Warning For detailed definitions of each status, see Status Definitions for Signaling Gateway Mated Pairs, page E-7.
Status Reason	Reason for the current status of the node. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons appear in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Signaling Points Table

The signaling points table displays information about the signaling points that the MWTM has discovered. To display the signaling points table, choose **Summary Lists > Signaling Points**. The signaling points table contains:

Column	Description
Internal ID	Internal ID of the signaling point. The internal ID is a unique ID for every object, which the MWTM assigns for its own internal use. It can also be useful when the TAC is debugging problems.
Name	Name of the signaling point.
Node	Name of the node associated with this signaling point.

Column	Description
Instance Number	Number of the instance associated with the signaling point.
Network Name	Name of the instance associated with the signaling point.
Point Code	Primary point code of the signaling point.
Variant	SS7 protocol variant. Valid variants are: • ANSI • China • ITU • NTT • TTC
Network Indicator	Determines the type of call that is being placed. Valid values are: • National—National-bound call. The MWTM routes national calls through the national network. • NationalSpare—National-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates the networks. • International—International-bound call. The MWTM forwards international-bound calls to an STP pair that acts as an international gateway. • InternationalSpare—International-bound call; used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates the networks.
Ignored	Indicates whether to include the signaling point when aggregating and displaying MWTM status information: • Uncheck the check box to include the signaling point. This is the default setting. • Check the check box to exclude the signaling point. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the signaling point.
Events (MWTM client only)	Indicates whether the signaling point has received any events. If the signaling point has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the signaling point.
Last Status Change	Date and time that the status of the signaling point last changed.
Severity	Indicates the alarm severity for the chosen signaling point. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.

Column	Description
Status	Current status of the signaling point. Possible values are:  Active  Unknown  Unmanaged  Warning For detailed definitions of each status, see Status Definitions for Signaling Points, page E-7.
Status Reason	Reason for the current status of the signaling point. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file resides at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file reside in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full status reason in a mouse over help popup. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Linksets Table

The linksets table displays information about the linksets that the MWTM has discovered. To display the linksets table, choose **Summary Lists > Linksets**.



Tip

Linksets that are associated with nodes that are excluded from the current view are not visible in the linksets table. See [Creating a New View, page 7-8](#), for more information about excluding nodes.

The linksets table contains:

Column	Description
Internal ID	Internal ID of the linkset. The internal ID is a unique ID for every object, which the MWTM assigns for its own internal use. It can also be useful when the TAC is debugging problems.
Name	Name of the linkset.

Column	Description
Node	Node associated with the linkset.
Signaling Point	Signaling point associated with the linkset.
Local Point Code	Point code of the primary signaling point for the linkset.
Adj Point Code	Point code of the adjacent signaling point for the linkset.
Linkset Type	Type of linkset, which the MWTM determines by examining the links defined in the linkset. Possible linkset types are: • HSL—The links in this linkset use the SS7-over-ATM high-speed protocol. • SCTPIP—The links in this linkset use the Stream Control TCP/IP transport protocol. • Serial—The links in this linkset use the serial SS7 signaling protocol. • Mixed—The links in this linkset are of two or more types. (This configuration is not recommended.) • Virtual—The links in this linkset are virtual links, which connect signaling point instances running on the same node. The MWTM does not poll virtual linksets, nor does it display real-time data or accounting statistics for virtual linksets. Note Prior to IOS release 12.2(23)SW1, the user manually created virtual linksets on multi-instance nodes. In and after that release, users can now automatically create virtual linksets. • Other—No links have been defined for this linkset.
Links	Total number of links in the linkset.
Active Links	Number of links in the linkset that are <i>Active</i> .
Congested Links	Number of links in the linkset that are <i>Congested</i> .
Ignored	Indicates whether to include the linkset when aggregating and displaying MWTM status information: • Uncheck the check box to include the linkset. This is the default setting. • Check the check box to exclude the linkset. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the linkset.
Events (MWTM client only)	Indicates whether the linkset has received any events. If the linkset has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the linkset.
Last Status Change	Date and time that the status of the linkset last changed.
Severity	Indicates the alarm severity for the chosen linkset. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.

Column	Description
Status	Current status of the linkset. Possible values are:  Active  Shutdown  Unavailable  Unknown  Warning For detailed definitions of each status, see Status Definitions for Linksets, page E-7.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Links Table

The links table displays information about the links that the MWTM has discovered. To display the links table, choose **Summary Lists > Links**. The links table contains:

Column	Description
Internal ID	Internal ID of the link. The internal ID is a unique ID for every object, which the MWTM assigns for its own internal use. This ID can also be useful when the TAC is debugging problems.
Node	Name of the node associated with the link.
Signaling Point	Name of the signaling point associated with the link.
Linkset	Name of the linkset associated with the link.
SLC	Signaling link code (SLC) ID for the link.
Type	Type of link. Possible link types are: • HSL—The link uses the SS7-over-ATM high-speed protocol. • SCTPIP—The link uses the Stream Control TCP/IP transport protocol. • Serial—The link uses the serial SS7 signaling protocol. • Virtual—The link is a virtual link, which connects signaling point instances running on the same node. The MWTM does not poll virtual links, nor does it display real-time data or accounting statistics for virtual links.
Congestion Level	Indicates the level of congestion on the link. A link is congested if it has too many packets waiting to be sent. This condition could result from the failure of an element in your network. Possible values for the Congestion Level field are <code>None</code> , indicating no congestion, and 1 to 3, indicating levels of congestion from very light (1) to very heavy (3).
Ignored	Indicates whether to include the link when aggregating and displaying MWTM status information: • Uncheck the check box to include the link. This is the default setting. • Check the check box to exclude the link. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the link.
Events (MWTM client only)	Indicates whether the link has received any events. If the link has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the link.
Last Status Change	Date and time that the status of the link last changed.
Severity	Indicates the alarm severity for the chosen link. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.

Column	Description
Status	Current status of the link. Possible values are:  Active  Blocked  Failed  InhibitLoc  InhibitRem  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Links, page E-6.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons appear in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Application Servers Table

The application servers table displays information about the application servers that the MWTM has discovered. To display the application servers table, choose **Summary Lists > App. Servers**. The application servers table contains:

Column	Description
Internal ID	Internal ID of the application server. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. This ID can also be useful when the TAC is debugging problems.
Name	Name of the application server.

Column	Description
Node	Name of the node associated with the application server.
Signaling Point	Name of the signaling point associated with the application server.
Protocol	Protocol associated with the application server. Possible values are: • M3UA—MTP3-User Adaptation. • SUA—SCCP-User Adaptation.
Routing Key	Routing key associated with the application server. The application server bases its routing decisions on the routing key value.
Traffic Mode	Method by which the application server forwards requests to its active application server processes. Possible values are: • overRide—One application server process takes over all traffic for the application server, possibly overriding any currently active application server process in the application server. • broadcast—Every active application server process receives the same message. • loadBind—Each application server process shares in the traffic distribution with every other currently active application server process, based on application server process bindings. • loadRndRobin—Each application server process shares in the traffic distribution with every other currently active application server process, using a round-robin algorithm. • undefined—The traffic mode is not defined. The first application server process that becomes active defines the traffic mode.
Application Server Process Associations	Total number of application server processes associated with the application server.
Active ASP Associations	Number of currently active application server processes associated with the application server.
Ignored	Indicates whether to include the application server when aggregating and displaying MWTM status information: • Uncheck the check box to include the application server. This is the default setting. • Check the check box to exclude the application server. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the application server.
Events (MWTM client only)	Indicates whether the application server has received any events. If the application server has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the application server.
Last Status Change	Date and time that the status of the application server last changed.
Severity	Indicates the alarm severity for the chosen application server. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.

Column	Description
Status	Current status of the application server. Possible values are:  Active  Down  Inactive  Pending  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Application Servers, page E-4.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Application Server Processes Table

The application server processes table displays information about the application server processes that the MWTM has discovered. To display the application server processes table, choose **Summary Lists > App. Server Processes**. The application server processes table contains:

Column	Description
Internal ID	Internal ID of the application server process. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. This ID can also be useful when the TAC is debugging problems.
Name	Name of the application server process.
Node	Name of the node associated with the application server process.

Column	Description
Local IP Address	Local IP address that the application server process is currently using.
Local Port	Local port number that the application server process is currently using.
Ignored	Indicates whether to include the application server process when aggregating and displaying MWTM status information: • Uncheck the check box to include the application server process. This is the default setting. • Check the check box to exclude the application server process. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the application server process.
Events (MWTM client only)	Indicates whether the application server process has received any events. If the application server process has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the application server process.
Last Status Change	Date and time that the status of the application server process last changed.
Severity	Indicates the alarm severity for the chosen application server process. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.
Status	Current status of the application server process. Possible values are:  Unknown  Unmanaged For detailed definitions of each status, see Status Definitions for Application Server Processes, page E-4.
Status Reason	Reason for the current status of the application server process. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Application Server Process Associations Table

The application server process associations table displays information about the application server process associations that the MWTM has discovered. To display the application server process associations table, choose **Summary Lists > App. Server Proc. Assoc.** The application server process associations table contains:

Column	Description
Internal ID	Internal ID of the application server process association. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. The ID can also be useful when the TAC is debugging problems.
Name	Name of the application server process association.
Node	Name of the node associated with the application server process association.
Signaling Point	Name of the signaling point associated with the application server process association.
Application Server	Name of the application server associated with the application server process association.
Protocol	Protocol associated with the application server process association. Possible values are: • M3UA—MTP3-User Adaptation. • SUA—SCCP-User Adaptation.
Congestion Level	Indicates the level of congestion of an application server process association. An application server process association is congested if it has too many packets waiting to be sent. This condition could result from the failure of an element in your network. Possible values for the Congestion Level field are None , indicating no congestion, and 1 to 7, indicating levels of congestion from very light (1) to very heavy (7).
Ignored	Indicates whether to include the application server process association when aggregating and displaying MWTM status information: • Uncheck the check box to include the application server process association. This is the default setting. • Check the check box to exclude the application server process association. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the application server process association.
Events (MWTM client only)	Indicates whether the application server process association has received any events. If the application server process association has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the application server process association.
Last Status Change	Date and time that the status of the application server process association last changed.

Column	Description
Severity	Indicates the alarm severity for the chosen application server process association. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.
Status	Current status of the application server process association. Possible values are:  Active  Blocked  Down  Inactive  Pending  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Application Server Process Associations, page E-4.
Status Reason	Reason for the current status of the application server process association. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first.
Status Reason (continued)	If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Signaling Gateway Mated Pairs Table

The signaling gateway-mated pairs table displays information about the signaling gateway-mated pairs that the MWTM has discovered. To display the signaling gateway-mated pairs table, choose **Summary Lists > Signaling Gateway Mated Pairs**. The signaling gateway-mated pairs table contains:

Column	Description
Internal ID	Internal ID of the signaling gateway-mated pair. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. The ID can also be useful when the TAC is debugging problems.
Name	Name of the signaling gateway-mated pair.
Mate	Name of the node associated with the mate of the signaling gateway-mated pair.
Node	Name of the node associated with the signaling gateway-mated pair.
Congestion Level	Indicates the congestion level of a signaling gateway-mated pair. A signaling gateway-mated pair is congested if it has too many packets waiting to be sent. This condition could result from the failure of an element in your network. Possible values for the Congestion Level field are None, indicating no congestion, and 1 to 7, indicating levels of congestion from very light (1) to very heavy (7).
Ignored	Indicates whether to include the signaling gateway-mated pair when aggregating and displaying MWTM status information: • Uncheck the check box to include the signaling gateway-mated pair. This is the default setting. • Check the check box to exclude the signaling gateway-mated pair. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the signaling gateway-mated pair.
Events (MWTM client only)	Indicates whether the signaling gateway-mated pair has received any events. If the signaling gateway-mated pair has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the signaling gateway-mated pair.
Last Status Change	Date and time that the status of the signaling gateway-mated pair last changed.
Severity	Indicates the alarm severity for the chosen signaling gateway-mated pair. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.

Column	Description
Status	Current status of the signaling gateway-mated pair. Possible values are:  Active  Down  Inactive  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Signaling Gateway Mated Pairs, page E-7.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOs/gm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Interfaces Table

The interfaces table displays information about the ITP or RAN interfaces that the MWTM has discovered. To display the interfaces table, choose **Summary Lists > Interfaces**. The interfaces table contains:

Column	Description
Internal ID	Internal ID of the interface. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. The ID can also be useful when the TAC is debugging problems.
Name	Name of the interface. The node specifies the name of the interface.
Node	Name of the node with the interface.
Interface Type	Type of interface.

Column	Description
Send Speed	Interface send speed in bits per second.
Receive Speed	Interface receive speed in bits per second.
Interface Index	Unique numeric identifier of the interface. This identifier appears in the interface table (ifTable).
Maximum Packet Size	The maximum packet size that traverses the interface in bytes.
Physical Address	The physical address of the interface. If a physical address does not apply to the interface, N/A appears in the table cell.
Ignored	Indicates whether to include the interface when aggregating and displaying MWTM status information: • Uncheck the check box to include the interface. This is the default setting. • Check the check box to exclude the interface. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the interface.
Events (MWTM client only)	Indicates whether the interface has received any events. If the interface has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the interface.
Last Status Change	Date and time that the status of the interface last changed.
Severity	Indicates the alarm severity for the chosen interface. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.
Status	Current status of the interface. Possible values are:  Active  Down  Inactive  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for RAN-O Interfaces, page E-8.
Admin Status	Desired state of the interface: • Up • Down • Testing • Shutdown For detailed definitions of each status, see Admin Status, page E-8.

Column	Description
Operational Status	Current operational state of the interface: • Up • Down • Testing • Unknown • Dormant • Not present • Lower layer down For detailed definitions of each status, see Operational Status, page E-8.
Status Reason	Reason for the current status of the interface. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOSgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip.
Status Reason (continued)	The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Cards Table

The cards table displays information about the cards in the ONS 15454 IPRAN node that the MWTM has discovered. To display the cards table, choose **Summary Lists > Cards**. The cards table contains:

Column	Description
Internal ID	Internal ID of the card. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. The ID can also be useful when the TAC is debugging problems.
Name	Name of the card. The node specifies the name of the card.
Node	Name of the node in which the card resides.
Card Type	Type of the card in the node.

Column	Description
Model Name	Model name of the card (can include the part number).
Description	Description of the card.
Slot Number	The slot number of the card in the node.
Ignored	Indicates whether to include the card when aggregating and displaying MWTM status information: • Uncheck the check box to include the card. This is the default setting. • Check the check box to exclude the card. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the card.
Events (MWTM client only)	Indicates whether the card has received any events. If the card has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the card.
Last Status Change	Date and time that the status of the card last changed.
Severity	Indicates the alarm severity for the chosen card. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.
Status	Current status of the card. Possible values are:  Active  Down  Inactive  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Cards, page E-10.

Column	Description
Status Reason	Reason for the current status of the card. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: - The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. - A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”
Hardware Version	Hardware version of the card.
Firmware Version	Firmware version of the card.
Software Version	Software version of the card.

RAN Backhauls Table

The RAN backhauls table displays information about the RAN backhauls that the MWTM has discovered. To display the RAN backhauls table, choose **Summary Lists > RAN Backhauls**. The RAN backhauls table contains:

Column	Description
Internal ID	Internal ID of the RAN backhaul. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. The ID can also be useful when the TAC is debugging problems.
Name	Name of the RAN backhaul.
Node	Name of the node on which this RAN backhaul resides.
Location	Location of the node (either at the cell site or the aggregation node site).
Peer Name	Name of the object's peer.
Peer Node	Name of the node to which the peer object belongs.
Type	Indicates whether the RAN backhaul is a normal backhaul or a virtual backhaul (see Creating Virtual RAN Backhauls, page 8-140).

Column	Description
User Send Bandwidth	The bandwidth that the user specified for the backhaul. Values for send and receive bandwidths will be different if the interface is asymmetrical. To change this value, see Editing Properties for a RAN-O Backhaul, page 6-36 .
User Receive Bandwidth	
System Send Bandwidth	The bandwidth that the system specifies for the backhaul. Values for send and receive bandwidths will be different if the interface is asymmetrical.
System Receive Bandwidth	
Ignored	Indicates whether to include the RAN backhaul when aggregating and displaying MWTM status information: • Uncheck the check box to include the RAN backhaul. This is the default setting. • Check the check box to exclude the RAN backhaul. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the RAN backhaul.
Events (MWTM client only)	Indicates whether the RAN backhaul has received any events. If the RAN backhaul has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the RAN backhaul.
Last Status Change	Date and time that the status of the RAN backhaul last changed.
Severity	Indicates the alarm severity for the chosen RAN backhaul. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.
Status	Current status of the RAN backhaul. Possible values are:  Active  Failed  Warning For detailed definitions of each status, see Status Definitions for RAN-O Backhauls, page E-10.

Column	Description
Status Reason	Reason for the current status of the card. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: - The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. - A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”
Accept Threshold ¹	The percentage threshold setting below which the backhaul utilization is considered acceptable.
Warning Threshold ¹	The percentage threshold setting beyond which the backhaul utilization issues a warning. Subsequent warnings are issued only if the utilization goes below the Acceptable Threshold.
Overload Threshold ¹	The percentage threshold setting beyond which the backhaul utilization is considered overloaded. Subsequent overload messages are issued only if the utilization goes below the Warning Threshold.

1. To change the default setting, see [Editing Properties for a RAN-O Backhaul, page 6-36](#).

RAN Shorthauls Table

The RAN shorthauls table displays information about the RAN shorthauls that the MWTM has discovered. To display the RAN shorthauls table, choose **Summary Lists > RAN Shorthauls**. The RAN shorthauls table contains:

Column	Description
Internal ID	Internal ID of the RAN shorthaul. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. The ID can also be useful when the TAC is debugging problems.
Name	Name of the RAN shorthaul.
Node	Name of the node to which the RAN shorthaul is connected.
Type	Type of shorthaul, either GSM or UMTS.

Column	Description
Optimized	Whether or not the traffic is optimized.
Location	Location of the node (either at the cell site or the aggregation node site).
Peer Name	Name of the object's peer.
Peer Node	Name of the node to which the peer object belongs.
Interface Type	Type of interface (for example, a point-to-point interface or an ATM interface).
Send Speed	Send speed of the interface in bits per second (for example, 1.98M).
Receive Speed	Receive Speed of the interface in bits per second (for example, 1.98M).
Interface Index	Unique numeric identifier of the interface. This identifier appears in the interface table (ifTable).
Maximum Packet Size (bytes)	Maximum packet size on the interface in bytes.
Physical Address	Physical address, if applicable, of the interface.
Ignored	Indicates whether to include the RAN shorthaul when aggregating and displaying MWTM status information: - Uncheck the check box to include the RAN shorthaul. This is the default setting. - Check the check box to exclude the RAN shorthaul. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the RAN shorthaul.
Events (MWTM client only)	Indicates whether the RAN shorthaul has received any events. If the RAN shorthaul has received an event, an icon appears in the table cell. Clicking the icon clears the event and takes you to the Recent Events tab for the RAN shorthaul.
Last Status Change	Date and time that the status of the RAN shorthaul last changed.
Severity	Indicates the alarm severity for the chosen RAN shorthaul. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.
Last Status Change	Date and time that the status of the shorthaul last changed.
Status	Current status of the RAN shorthaul. For detailed definitions of each status, see Status Definitions for RAN-O Backhauls, page E-10.
Admin Status	Desired state of the interface: - Up - Down - Testing - Shutdown For detailed definitions of each status, see Admin Status, page E-8.

Column	Description
Operational Status	Current operational state of the interface: • Up • Down • Testing • Unknown • Dormant • Not present • Lower layer down For detailed definitions of each status, see Operational Status, page E-8.
Status Reason	Reason for the current status of the card. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOSgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Access Point Names Table

The RAN shorthauls table displays information about the RAN Access Point Names that the MWTM has discovered. To display the Access Point Names table, choose **Summary Lists > Access Point Names**. The Access Point Names table contains:

Column	Description
Internal ID	Internal ID of the RAN shorthaul. The internal ID is a unique ID for every object, that the MWTM assigns for its own internal use. The ID can also be useful when the TAC is debugging problems.
Name	Name of the RAN shorthaul.
Index	The Index assigned to the access point.

Column	Description
Ignored	Indicates whether to include the RAN shorthaul when aggregating and displaying MWTM status information: • Uncheck the check box to include the RAN shorthaul. This is the default setting. • Check the check box to exclude the RAN shorthaul. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the RAN shorthaul.
Severity	Indicates the alarm severity for the chosen RAN shorthaul. The severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, Unmanaged, or Normal. See Managing Alarms and Events, page 9-1 for more information.
Last Status Change	Date and time that the status of the shorthaul last changed.
Status	Current status of the RAN access point: For detailed definitions of each status, see Status Definitions for APNs, page E-10.
Status Reason	Reason for the current status of the card. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: • The default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • A different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears first. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Software Versions Table

The Software Versions table lists the software versions for each node the MWTM manages. This option is Web-only and does not appear in the MWTM client.

For details on the Software Versions table, see [Displaying Software Versions, page 11-31](#).

Point Codes

You can view current point code inventory reports using the MWTM. You can also export the reports.

Current Point Code Inventory

The Point Codes Report page shows all point codes that are currently being used by all nodes that the MWTM detected.

The MWTM shows the Point Codes Report page.

The Point Codes Report table is sorted based on the information in the Node column. However, you can sort the table based on the information in any of the columns (see [Navigating Table Columns, page 5-24](#)).

Field or Column	Description
Signaling Point	Signaling point that is currently being used by a node. To sort the point codes by signaling point in descending order, click the Signaling Points heading. Click again to sort the point codes in ascending order.
Point Code	Point code that is currently being used by a node. To sort the point codes by point code in ascending order, click the Point Codes heading. This is the default display. Click again to sort the point codes in descending order.
Node	Name or IP address of the node. To see more information for the node, click the node name. To sort the point codes by node in descending order, click the Node heading. Click again to sort the point codes in ascending order.
Point Code Type	Type of point code: • Primary—Main point code used by a node. • Secondary—Alternate or backup point code used by a node. • Capability—Shared by more than one node, each of which is also assigned a real point code. Also called an alias point code. To sort the point codes by type in ascending order, click the Point Code Type heading. Click again to sort the point codes in descending order.

IP Addresses

You can view a report of IP addresses of the nodes that the MWTM manages. You can also export this report to a CSV file. The IP Addresses report contains:

Field or Column ¹	Description
Node	Name or IP address of the node. To see more information for the node, click the node name. Note Each node can be associated with one or more IP addresses.
IP Address	IP address of the node.
Last Regular Poll Interval	The last time this node was polled.
SNMP Pollable	Whether the node can be polled by SNMP (yes or no).

1. To sort the column in descending order, click the column heading. Click again to sort the list in ascending order.

Editing Properties

In the Edit Properties dialog box you can change the basic properties associated with these objects:

- Views
- Nodes
- Signaling Points (ITP only)
- Application Server Processes (ITP only)
- Backhauls (RAN-O only), (see [Editing Properties for a RAN-O Backhaul, page 6-36](#))

Example:

To edit a node's properties, right-click the node in the Node table in the right pane or in a view in the navigation tree, and choose **Edit > Properties** in the right-click menu. The MWTM displays the Edit Properties dialog box.

The Edit Properties dialog box contains:

Field or Button	Description
Name	Name of the object. • For application server processes only—This field cannot be edited. • For nodes only—By default, this field displays the node's DNS name, which the MWTM discovered. However, if you modified your preferences to identify nodes by their IP addresses, then that is how the node is identified in this field. For more information, see Node Name Settings, page 5-5. • For signaling points only—By default, this field displays the signaling point's point code and network name, which the MWTM discovered (for example, 1.22.0:net0). You can also use this field to specify a new, more meaningful name for the node or ITP signaling point. Remember that: • You can change an object's name to a new name or IP address. • A new name can be from 1 to 30 characters, and can contain any letters (upper- or lowercase) and any numbers, as well as blank spaces (), hyphens (-), and underscores (_), but no periods (.). If you enter a name that is longer than 30 characters, or if you enter any other special characters or periods, the MWTM beeps and retains the current name. • If you enter a name that includes a period (.), the MWTM assumes that you are entering a new IP address. A new IP address must use the <i>x.x.x.x</i> format, where <i>x</i> is between 0 and 255, and must contain only numbers and periods (.), but no letters or special characters. If you enter an IP address that contains any letters or special characters, the MWTM beeps and retains the current IP address.

Field or Button	Description
Name (continued)	- If you edit an object whose current name already contains invalid characters, the MWTM beeps and replaces the name with blanks. Enter a new name that uses only valid characters, or click Cancel to keep the existing name. If you click Cancel, the MWTM exits the Edit Properties dialog box without saving any changes to the Name, Connect Address, or Icon Name field. - If you leave the Name field blank, the MWTM reverts to the object's default name (dependent upon network type). - The new object's name <i>is</i> used when launching context-based applications, such as CiscoWorks. Therefore, if the new name that you enter is not the object's DNS name, and the application knows the object by its DNS name, context links into the application for that object might not work. When you click Save, all MWTM windows are updated automatically to reflect the new name.
Connect Address (Nodes only)	Connect IP address to pass to the Telnet or SSH command. A new Telnet or SSH IP address must use the <i>x.x.x.x</i> format, where <i>x</i> is between 0 and 255, and must contain only numbers and periods, but no letters or special characters. If you enter a Telnet or SSH IP address that contains any letters or special characters, the MWTM beeps and retains the current IP address.
Connect Port (Nodes only)	Optional port number to pass to the Telnet or SSH command.
Icon Name	Drop-down menu of graphic icons to assign to this object in topology maps. The MWTM automatically assigns an appropriate icon to each discovered node and to Unknown nodes; but, you can use this field to assign a different icon (for example, if you know that a given Unknown node is a mobile switching center). Note Additional icon types appear in the list for user customization. When the MWTM discovers a single-instance node, it assigns the icon that corresponds to the node. When the MWTM discovers a multi-instance node, it assigns a separate icon for each unique instance. Icon names include the following: - ASP—Application server process - BSC—Base Station Controller ¹ - BTS—Base Transceiver Station ¹ - Building—Icon representing a collection of network objects in a building. - Cisco2600—Cisco 2650, Cisco 2650XM, Cisco 2651, Cisco 2651XM - Cisco2800 - Cisco3845 - Cisco7202, Cisco7204 (Cisco 7204, Cisco 7204VXR), Cisco7206 (Cisco 7206, Cisco 7206VXR) - Cisco7301, Cisco7304 - Cisco7505, Cisco7507 (Cisco 7507, Cisco 7507mx, Cisco 7507z), Cisco7513 (Cisco 7513, Cisco 7513mx, Cisco 7513z)

Field or Button	Description
Icon Name (continued)	• Cisco 7600—Cisco 7603, Cisco 7603s, Cisco 7604, Cisco 7606, Cisco 7606s, Cisco 7609, Cisco 7609s, Cisco 7613 • CiscoMWR1900—Cisco Mobile Wireless Router 1900 • City—Icon representing a collection of network objects in a city. • Cloud—Collection of network objects, called a submap. A submap can also contain other submaps. • Database—Icon representing a database object. • IPDevice—IP device, other than those listed previously. • MatedPair—Mated pair of signaling points • MSC—Mobile switching center. • Node B—The radio transmission/reception unit for communication between radio cells ¹ • PGW—Cisco Public Switched Telephone Network (PSTN) Gateway (PGW) 2200 Softswitch • RAN_SVC—RAN Service Module in the Cisco ONS 15454 • RNC—Radio Network Controller ¹ • SCP—Service control point • SignalingPoint—An SCP, SSP, or STP, or an ITP instance • SSP—Service switching point • STP—Signal transfer point • Tower—Icon representing a PC tower. • TrafficGenerator—Icon representing a device or emulator used to generate traffic, usually in a test environment. • Unknown—The MWTM is unable to determine the node or signaling point type. • Workstation—Icon representing a workstation. • Workstation2—Icon representing a different workstation. When you click Save, the topology window is updated automatically to reflect the new icon.

Field or Button	Description
Interface Structure	Drop-down menu to configure the way the MWTM displays the physical interfaces of a node (excluding the ONS node). Choices include: - Default—Restores the interface structure to the default setting for the node. For example, if the default structure is hierarchical, choosing this option restores the parent-child hierarchy in the Physical folder. Note In cases where the MWTM cannot determine the interface hierarchy of a node, the MWTM sets its default structure to be flat (that is, all interfaces appear at the same level). - Force Flat—Forces the interface structure of a node to be flat (that is, no hierarchy). All interfaces in the Physical folder appear at the same level. - Force Hierarchical—Forces the interface structure of a node to be hierarchical (that is, to display parent-child relationships among interfaces). When you choose a different setting, the MWTM opens a popup with this message: A clean poll will be triggered if this value is changed. Click OK to close the popup. Click Save to activate your changes. You can view your changes in the MWTM client and web interfaces.
Save	Button to save the changes that you make to the object information. Updates all MWTM windows to reflect your changes, and exits the dialog box.
Restore	Button to restore changes that you make to the Name and Icon Name fields of the Edit Properties dialog box and leave the dialog box open.
Cancel	Button to exit the dialog box without saving any changes.
Help	Button to display online help for the dialog box.

1. The MWTM does not manage BSC, BTS, RNC, or Node B objects but displays them in the topology window to help you visualize the network.

Editing Properties for a RAN-O Backhaul

To edit the properties of a backhaul or virtual backhaul interface, right-click the backhaul object in the navigation tree or right pane, and choose **Edit > Properties** in the right-click menu.

The MWTM displays the Edit RAN Backhaul Properties dialog box.

The Edit RAN Properties dialog box contains:

Field or Button	Description
Name	Name of the backhaul. You can use this field to specify a new, more meaningful name for the backhaul. Remember that: - You can change a backhaul's name to a new name. A new name can contain: - From 1 to 30 characters - Any letters (upper- or lowercase) - Any numbers, as well as blank spaces (), dashes (-), underscores (_), or periods (.) If you enter a name that is longer than 30 characters, or if you enter any other special characters, the MWTM beeps and retains the current name. - If you edit an object whose current name already contains invalid characters, the MWTM beeps and replaces the name with blanks. Enter a new name that uses only valid characters, or click Cancel to keep the existing name. If you click Cancel, the MWTM exits the Edit RAN Backhaul Properties dialog box without saving any changes to the Name, Connect Address, or Icon Name field. When you click Save, all MWTM windows are updated automatically to reflect the new name.
Threshold Information	Pane that displays three slider bars for controlling the Acceptable, Warning, and Overloaded threshold settings. Left-click the slider and drag it to the desired setting for each threshold. See Threshold Information (RAN-O Only), page 8-43, for descriptions of these thresholds.

Field or Button	Description
Bandwidth Information	Pane that displays: • User Send Bandwidth (bits/sec) • User Receive Bandwidth (bits/sec) The user bandwidth is the value that you (the user) specify for the backhaul. Send and receive values will differ if the interface is asymmetrical. The backhaul utilization appears in the backhaul real-time chart as a percentage of the User Bandwidth. The preset value for the User Bandwidth is the same as the System Bandwidth. When you change the User Bandwidth, you are changing the scale of the Y axis of the backhaul real-time chart in the Performance tab (see Viewing Backhaul Performance Data, page 8-111). The X and Y values of the data do not change. The threshold ranges resize because they are percentages of User Bandwidth. The User Bandwidth represents 100% utilization. Data points that are higher than the User Bandwidth will exceed 100% utilization. The Y axis dynamically increases to display all data points. (See Why does my backhaul utilization graph show greater than 100% for transmit traffic?, page C-22.) • System Send Bandwidth (bits/sec) • System Receive Bandwidth (bits/sec) The system bandwidth is the value that the system specifies for the backhaul. Send and receive values will differ if the interface is asymmetrical. You cannot edit this field.
Save	Saves changes that you make to the object information, updates all MWTM windows to reflect your changes, and exits the dialog box.
Restore	Restores changes that you make to the Name, and sets the Threshold Information, and Bandwidth Information fields to the system defaults. The dialog box is left open.
Cancel	Exits the dialog box without saving any changes.
Help	Displays online help for the dialog box.

Attaching Notes



Tip

Users with East Asian Languages configured on Windows are supported.

You use the MWTM to annotate an object, attaching a descriptive string to it. To attach a note to an object, in the:

- MWTM client, right-click the object in the navigation tree, then choose **Edit > Notes**. The Edit Notes dialog box appears.
- Web interface, left-click the object in the navigation tree, click the Notes tab, then click **Edit**. The text area becomes active.

**Note**

You can add a note to a node by using either the MWTM client or the web interface. You can also view the note from either interface.

The Edit Notes dialog contains:

Field or Button	Description
Name	Name of the object. You cannot edit this field.
Note Last Updated	Date and time the Notes field for this object was last updated. If no note is currently associated with this object, this field displays the value <code>Not Set</code> . You cannot edit this field.
Notes	Notes to associate with this object. In this field, you can enter any important information about the object, such as a detailed description, location, service history, and so on.
Edit	(Web interface only) Enables you to edit or add a note in the content area.
Save	Saves changes that you make to the object's notes, updates all MWTM windows to reflect your changes, and closes the dialog box. When you annotate an object, the MWTM displays a note icon in the Notes column of all object tables for the annotated object, and the topology map in the topology window displays a note icon in the upper-left corner of the object.
Cancel	Cancels the operation without saving any changes.
Help	Displays online help for the dialog box.

Viewing Notes

You use the MWTM to view any notes that are associated with an object. To view a note:

- Select an object in the navigation tree, then click the Notes tab.
- Right-click an object in a window, then choose **View > Notes**. (The Notes option is dimmed if no note is associated with the chosen object.)

The MWTM displays the Notes tab for the chosen object, which shows:

- Notes associated with the object.
- The date and time the notes associated with the object were last updated, or the message `Not Set` if no notes are associated with the object.
- The message `No Notes` if no notes are associated with the object.

**Note**

The Notes tab is not supported on the DEFAULT View in the web interface.

Example:

To view a note for a node, right-click the node in the Node table in the right pane or in a view in the navigation tree, then choose **View > Notes** in the right-click menu.

Deleting Objects

After discovery, the objects in your network are known to the MWTM and added to the MWTM database. Physically deleting objects from your network is not the same as deleting them from the MWTM database. These sections describe the differences between deleting objects from your network, the MWTM database, and the MWTM discovery database, and the procedures for doing so:

- [Deleting an Object from Your Network, page 6-40](#)
- [Deleting an Object from the MWTM Database, page 6-40](#)

Deleting an Object from Your Network

If you physically delete a known object from your network (for example, by powering down a node), it remains in the MWTM database, the MWTM labels it Unknown, and the system administrator is responsible for deleting it from the MWTM database, if you choose to do so.



Note

For nodes, the MWTM also labels all associated network objects Unknown because the MWTM attempts to poll the node and gets no response. For details on polling nodes, see [Polling a Node, page 8-53](#).

Deleting an Object from the MWTM Database

Typically, you delete an object from the MWTM database for one of these reasons:

- You physically deleted the object from your network. This is the most common reason for deleting a object from the MWTM database.
- The object state is one of these:

Object	States	Applicable To
Node	Unknown, Unmanaged	ITP and IP-RAN networks
Interface	Unknown	
Signaling Point	Unknown, Unmanaged	ITP networks only
Linkset	Unknown	
Link	Unknown	
Application Server	Unknown	
Application Server Process	Unknown	
Application Server Process Association	Unknown	
Signaling Gateway Mated Pair	Unknown	

You are aware of the reason for the state, and you no longer want to see the object in the MWTM displays. For example, the object might be a test lab device, or it could be associated with an object that was removed from the network.

**Note**

If an object has at least one adjacent object in Active, Discovering, Waiting, or Warning state, you cannot delete the object. If you try, the MWTM cancels the deletion.

- If you delete all associated connections to an Unmanaged object, the MWTM does not automatically delete the object. Instead, you must manually delete the object.

If you have physically deleted a known object from your network, and you then delete it from the MWTM, it is no longer in the MWTM database, it does not appear in MWTM windows, and it is not discovered when you run discovery.

If you have *not* physically deleted a known object from your network, and you delete it from the MWTM, any associated objects are also automatically deleted from the MWTM database (if applicable). However, at the next poll the MWTM finds the object (and any associated objects) and adds it back to the MWTM database, setting the status appropriately. If this happens, do not delete the object again. Instead, set it to Ignored. See [Ignoring and Unignoring Objects, page 6-43](#), for more information.

To delete an object from the MWTM database, use one of these procedures:

**Note**

If you delete an object from the MWTM database, the object is deleted for all MWTM clients and views that are connected to that MWTM server.

- Select one or more objects in a window, then choose **Edit > Delete** from the MWTM main menu.
- Right-click the object in a window, then select **Delete** from the right-click menu. (You cannot delete more than one object at a time from the right-click menu.)

The MWTM asks you to confirm the deletion. Click:

- **Yes** to delete the chosen objects. The MWTM deletes the objects from the MWTM database.
- **No** to return to the window without deleting any objects from the MWTM database.

You can also enter the **mwtm delete** commands from the command line interface to delete one or more objects from the MWTM database. See [mwtm delete, page B-23](#), for more information on the use of this command.

Deleting a Node from the MWTM Discovery Dialog

If you want to completely eliminate a given node from the MWTM database, you can delete it from the MWTM Discovery dialog box, ensuring that the MWTM never even discovers it.

**Note**

If you delete a node from the MWTM Discovery dialog box, the node is deleted for *all* MWTM clients and views connected to that MWTM server.

To delete a node from the MWTM Discovery dialog box:

- Step 1** Choose **Network > Network Discovery** from the MWTM main menu. The Discovery dialog box appears.
- Step 2** Click the **Discovery** tab.
- Step 3** In the Discovered Nodes table, select the node that you want to delete.
- Step 4** Click **Delete Node**.

The MWTM deletes the nodes from the MWTM database, without asking for confirmation. The MWTM will no longer discover the nodes.

Unmanaging and Managing Nodes or ITP Signaling Points

You use the MWTM to change a node or any associated signaling point to the Unmanaged state. You can also remove the Unmanaged state from these objects.

In some situations, you might not want a node or signaling point to appear in MWTM windows. However, you might be unable to delete the object from the MWTM database. For example, if:

- You have not physically deleted a known node or signaling point from your network, and you delete it from the MWTM, the object is removed from the poll list. However, at the next poll, the MWTM returns the object to the DEFAULT view. If you are using a custom view, the MWTM labels the object as new.
- A node has at least one adjacent node in Active, Discovering, Waiting, or Warning state; or, if a signaling point has at least one adjacent signaling point in Active or Warning state, you cannot delete the node or signaling point. If you try, the MWTM cancels the deletion.

In these situations, you can label the object as Unmanaged. When you set a node or signaling point to the Unmanaged state, the MWTM removes the object from the poll list.



Note

If you change a node or signaling point to the Unmanaged state, the object is Unmanaged for all MWTM clients and views connected to that MWTM server.

To label a node or signaling point Unmanaged:

Step 1 Choose the node or signaling point in a window.



Note

You cannot label a node Unmanaged if it has a Node Type of Unknown. If you select a node with a Node Type of Unknown, this menu option is dimmed and cannot be chosen. If you select more than one node, and at least one of them has a Node Type of Unknown, this menu option is grayed-out and cannot be chosen.

Step 2 Select **Unmanage** from the right-click menu. The MWTM labels the chosen node and any associated signaling point(s) Unmanaged and removes them from the poll list.



Note

When you set a node or signaling point to the Unmanaged state, the events for the object will continue to appear in the Events window. If you want to suppress events for unmanaged objects, see [Setting an Alarm or Event Filter, page 9-18](#).

You can also remove the Unmanaged status from a node or signaling point, when you are ready to return them to the MWTM poll list. To remove the Unmanaged status from an object:

Step 1 Select the node or signaling point in a window.

**Note**

You cannot remove the Unmanaged status from a node with a Node Type of Unknown. If you select a node with a Node Type of Unknown, then this menu option is dimmed and cannot be chosen. If you select more than one node, and at least one of them has a Node Type of Unknown, then this menu option is grayed-out and cannot be chosen.

Step 2

Select **Manage** from the right-click menu. The MWTM removes the Unmanaged status from the chosen node, returns it to the poll list, and polls it immediately.

**Note**

(ITP only) You can also remove the Unmanaged status from a signaling point, when you are ready to return the signaling point to the MWTM poll list. To remove the Unmanaged status from a signaling point, right-click a signaling point in a window, then select **Manage Node** from the right-click menu. The MWTM removes the Unmanaged status from the chosen signaling point, the node associated with the signaling point, and all other signaling points associated with that node. The MWTM then returns these objects to the poll list, and polls them immediately.

Excluding Nodes or ITP Signaling Points from a View

To exclude a node or signaling point from the current view, right-click the node or signaling point in a window, then select **Exclude from View** in the right-click menu. The MWTM excludes the node or signaling point from the current view. See [Creating a New View, page 7-8](#), for more information about excluding objects from views.

Ignoring and Unignoring Objects

You can instruct the MWTM to ignore an object when it aggregates and displays network data. Setting objects to Ignored prevents known problems from affecting MWTM displays for associated network objects. In effect, you are preventing a known problem from distracting you from other, more urgent network problems.

Example:

You can set a node to Ignored before shutting down the node for maintenance.

**Note**

If you set an object to Ignored, the object is ignored for all MWTM clients and views connected to that MWTM server.

Also, if you set an object to Ignored, make a note of the change, and remember to reset the object when the problem is corrected or the maintenance is complete.

- To set an object to Ignored:

Right-click the object, then select **Ignore** from the menu

or

In the object window in the right pane, check the **Ignored** check box.

- To display all objects that are ignored in the object window, click the Ignored column heading. The MWTM displays all ignored objects at the top of the table.
- To set an object to ignore in the topology window, select an object in the topology map, then, in the left pane, select the **Ignored** check box for the object you want to ignore.
- To unignore an object, right-click the object, then select **Unignore** from the menu.



CHAPTER 7

Managing Views



Note

The web interface does not support the views feature. You can create customized views only in the Cisco Mobile Wireless Transport Manager (MWTM) client interface.

This section contains:

- [Overview, page 7-1](#)
- [Viewing Basic Information for Custom Views, page 7-2](#)
- [Viewing Detailed Information for Views, page 7-5](#)
- [Editing a View, page 7-6](#)
- [Saving a View, page 7-6](#)
- [Creating a New View, page 7-8](#)
- [Loading the DEFAULT View, page 7-14](#)
- [Loading a Client-Specific View, page 7-15](#)
- [Ignoring a View, page 7-16](#)
- [Viewing Ignored Views, page 7-16](#)

Overview

This chapter describes how to create and manage multiple views of your network from the MWTM client. Before creating or managing a view, you must understand the basic concepts of a default view, a custom view (and its associated subviews), and the navigational features available in each view:

- [Default View, page 7-2](#)
- [Custom View and Subviews, page 7-2](#)
- [Viewing Basic Information for Custom Views, page 7-2](#)

Default View

When the Cisco Mobile Wireless Transport Manager (MWTM) discovers your network, all discovered objects are placed in a DEFAULT view, which is stored on the MWTM server and shared by all MWTM clients. Clients cannot modify the DEFAULT view that is stored on the MWTM server. This view is always available for users who need to view the entire network.

Initially, all clients use the DEFAULT view. However, you can use the MWTM to create your own, client-specific views and subviews, which are subsets of the DEFAULT view, to meet your individual needs.

Custom View and Subviews

You can choose the nodes you are interested in managing, exclude all other nodes from your view, and change the layout of the topology map in the topology window. You can save all of this customized information in a custom view and set that view as the new *default* view for the MWTM client.

You can use the MWTM client from then on to manage only the part of the network you are interested in, with the settings you prefer. When you modify the DEFAULT view in any way (except for modifying the layout of the topology map in the topology window), the MWTM prompts you to name the new, custom view.

You can also create many different views and subviews on a given MWTM client, with each view devoted to a different aspect of the network. You can then load a different view to manage a different part of the network, or switch to the DEFAULT view to see the entire network. For details on creating views, see [Creating a New View, page 7-8](#).

If more than one person uses a certain MWTM, each user can create a personal view.

Also, you can create subviews in any custom view. The custom view becomes the parent view of one or more subviews. When you load a custom view that has subviews, the MWTM displays the Views label under Summary Lists in the navigation tree. When you click Views, the Views table appears in the right pane and lists all subviews of the custom (parent) view (see [Views Summary List Table, page 7-3](#)).

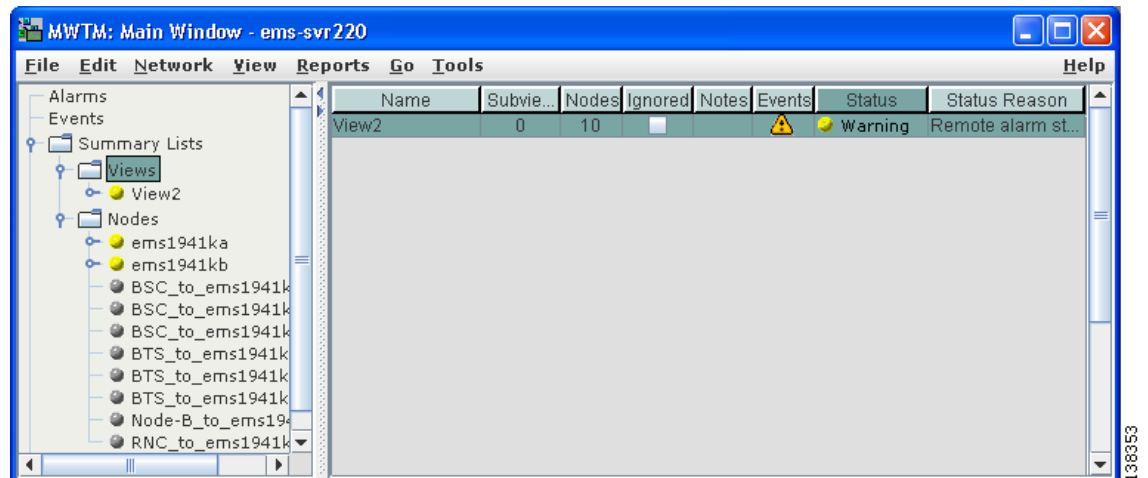
**Note**

You cannot create subviews for the DEFAULT view. Subviews are valid only for custom views.

Viewing Basic Information for Custom Views

To see all subviews currently configured in a custom view:

-
- Step 1** Load a custom view by choosing **File > Load View**.
 - Step 2** Choose a custom view from the View List in the Load File dialog box and click **OK**.
If the chosen custom view has associated subviews, the Views label appears under Summary Lists in the navigation tree.
 - Step 3** Click the turner  beside **Summary Lists**, then click **Views**.
The View Summary List window appears.
-

Figure 7-1 View Summary List Window

The View Summary List window provides information about all subviews that have been defined for this custom view, including their status and other important information.

The View Summary List window contains these sections:

- [Right-Click Menu for Views, page 7-3](#)
- [Views Summary List Table, page 7-3](#)

Related Topics:

- [Viewing Detailed Information for Views, page 7-5](#)
- [Navigating Table Columns, page 5-24](#)

Right-Click Menu for Views

To see the right-click menu for views, under Summary Lists, select **Views** and right-click the mouse. For details on menu options, see [Viewing the Right-Click Menu for an Object, page 8-3](#).



Note

If the Views label does not appear under Summary Lists, you have loaded the DEFAULT view or a custom view that has no subviews.

Views Summary List Table

The views table shows information about the subviews that have been defined for a custom view. If a custom view has no subviews, this option is not available.

You can resize each column, or sort the table based on the information in one of the columns. By default, this table is sorted by Parent View, and the MWTM shows all of the columns in the view table except Internal ID.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The view table contains:

Column	Description
Internal ID	Internal ID of the view. The internal ID is a unique ID for every object, assigned by the MWTM for its own internal use. It can also be useful when the TAC is debugging problems.
Name	Name of the subview that belongs to the custom (parent) view.
Parent View	Name of the custom or parent view to which the subview belongs.
Ignored	Indicates whether the subview should be included when aggregating and displaying MWTM status information: • Check the check box to ignore the subview. • Uncheck the check box to include the subview. This is the default setting. Users with authentication level Power User (level 2) and higher can edit this field.
Notes	Indicates whether a note is associated with the subview.
Events	Indicates whether a recent event associated with a network object in the subview. (Even if the server purges all of the events associated with objects in the subview, the MWTM continues to display the event icon in this field.) To delete the event icon (orange triangle) from MWTM displays for: • A specific subview, select the subview and click the icon. • All subviews, choose Edit > Clear All Events from the MWTM main menu. Note During Discovery, the MWTM might flag most views with an event icon. If the event icons are too distracting, use the Edit > Clear All Events menu option to remove them. Changing a view (for example, by ignoring it or attaching a note to it) does not generate an event, and therefore does not cause an event icon to appear in this field. Deleting an application server process, node, or signaling point with the Delete menu option does not generate an event, and therefore does not cause an event icon to appear in this field. However, if the MWTM rediscovers a deleted application server process, node, or signaling point, events are generated and logged for the deletion and the rediscovery, and the event icon appears in this field.
Last Status Change	Date and time that the status of the subview last changed.
Severity	This is the worst severity of the network objects in the view or any subview.

Column	Description
Status	Current status of the subview. Possible values are:  Active  Unmanaged  Warning For detailed definitions of each status, see Appendix E, “Status Definitions.”
Status Reason	Reason for the current status of the subview. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed the MWTM in: - The default directory, <i>/opt</i>, then the file resides at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. - A different directory, then the help directory and file reside in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.”

Viewing Detailed Information for Views

The MWTM can display detailed information about a chosen view, including its associated objects, status, and other information.

Updates for the view that are received from the MWTM server are reflected automatically in this window.

To display the Details tab for a view, click the name of the view in the MWTM main window navigation tree. For example, to see detailed information for the DEFAULT view in the right pane, click DEFAULT View in the navigation tree.

The View Details window contains:

Function or Tab	For More Information
Right-click menu (MWTM client only)	Viewing the Right-Click Menu for an Object, page 8-3.
Status Contributors	Viewing Status Contributors, page 8-10
Details	Viewing Details, page 8-12

Function or Tab	For More Information
Notes (MWTM client only)	Viewing Notes, page 6-39
Recent Events	Viewing Alarms and Recent Events, page 8-45
Alarms	Viewing Alarms and Recent Events, page 8-45

Editing a View

For details on editing a view, see [Editing Properties, page 6-33](#).

Saving a View

You use the MWTM to save a specific view, change the list of views, and select one view to be loaded automatically when the associated preferences file is saved.

When you are satisfied with the changes you made to a view, use one of these procedures to save the view:

- To save the changes you made to the view without changing the name of the file, choose **File > Save** from the View Editor window menu.



Note You cannot save changes to the DEFAULT view. If you are currently using the DEFAULT view and you choose **File > Save**, the MWTM shows the Save File Dialog: View List dialog box.

- To save the changes you made to the view with a new name, choose **File > Save As** from the Discovery Dialog menu. The MWTM shows the Save File Dialog: View List dialog box.

The MWTM stores the view in the view file directory on the MWTM server:

- If you installed the MWTM in the default directory, */opt*, then the MWTM view file directory is */opt/CSCOsgm/views*.
- If you installed the MWTM in a different directory, then the MWTM view file directory resides in that directory.



Note If another user modifies and saves the view before you save your changes, the MWTM asks if you want to overwrite that user's changes. If you choose to do so, the other user's changes are overwritten and lost. If you choose not to do so, your changes are lost, unless you save the view to a different filename.

The Save File Dialog: View List contains:

Field or Button	Description
 Create New Folder	Click this icon to create a new folder in the current directory. This action opens the Input dialog box. Enter a folder name and click OK. The new folder appears in the Save File dialog box. Double-click the folder to open it. You can save files in this folder or create another folder at this level.
 Go Up One Folder	Click this icon to go up one folder in the directory structure.
Type	Icon indicating whether the item in the table is a file or a folder.
Name	Name of the view file or folder.
Last Modified	Date and time the view file or folder was last modified.
Size (bytes)	Size of the view file or folder, in bytes.
Filename	Name by which you want to save the view. You must specify a name other than DEFAULT view. You cannot save changes to the DEFAULT view. When you create a new view filename, you can use any letters, numbers, or characters in the name that are allowed by your operating system. However, if you include any spaces in the new name, the MWTM converts those spaces to dashes. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i>.
Make this my preferred startup option	Specifies whether the chosen view should be loaded automatically whenever the associated preferences file is loaded. To load the: • Saved view, select the view, then check this check box. • Last-used view, uncheck the check box. This is the default setting.
OK	Saves any changes you made to the current named view or to the list of views and closes the dialog box. To save the view with a new name, use one of these procedures. To save the file with: • A completely new name, enter the new name and click OK. • An existing name, overwriting an old view, select the name in the list and click OK. The MWTM saves the view with the new name, closes the Save File Dialog: View List dialog box, and returns to the Discovery dialog box. To save any changes you made to the list of files, click OK. The MWTM saves the changes and closes the Load File Dialog: View List dialog box.

Field or Button	Description
Delete	Deletes the chosen file from the view list. The MWTM issues an informational message containing the name and location of the deleted file.
Cancel	Closes the dialog box without saving the view or any changes to the view list.
Help	Shows online help for the dialog box.
Number of Files (visible in bottom left corner)	Total number of view files and folders.

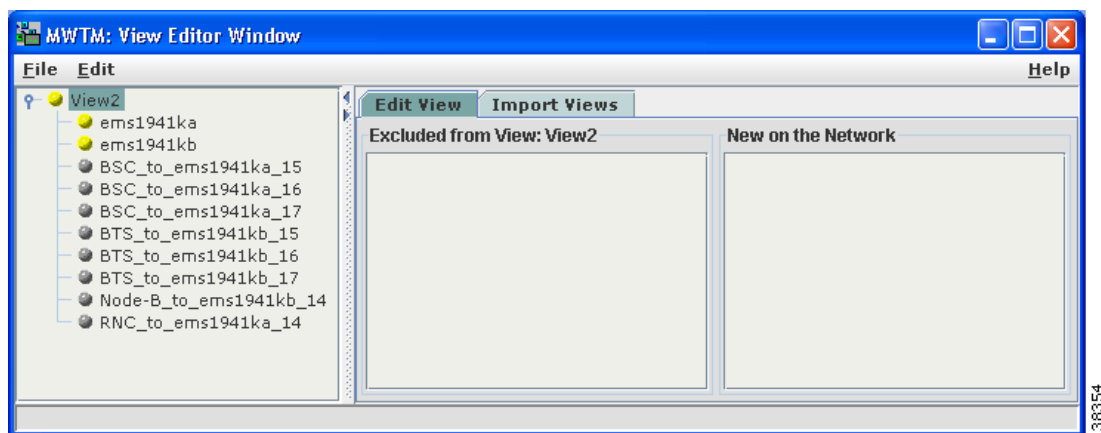
Creating a New View

You use the MWTM to specify the nodes and objects you want to see in MWTM displays. This view is called a client-specific network view. All changes you make are reflected in topology tables and maps as soon as you make the changes.

Before creating a client-specific network view, ensure that Discovery has been run at least once, and data appears in the server's MWTM database. See [Discovery Overview, page 4-4](#), for details.

To create a client-specific network view, choose **Edit > Views** from the MWTM main menu. The View Editor window appears.

Figure 7-2 View Editor Window



The View Editor window shows two tabs:

- The Edit View tab provides:
 - All objects that are in the current view.
 - All objects that have been excluded from the current view.
 - New objects that the MWTM found.
- The Import Views tab provides:
 - All views currently defined on this MWTM client.
 - Data about the views.

You use the View Editor window also to move objects into and out of the current view. All changes that you make in this window are reflected in the MWTM client, and in the topology tables and maps as soon as you make the changes.

The View Editor window contains:

- [View Editor Window Menu, page 7-9](#)
- [Objects In Current View, page 7-10](#)
- [Excluded from View Pane, page 7-12](#)
- [New on the Network Pane, page 7-12](#)
- [Views List Pane, page 7-13](#)
- [View Data Pane, page 7-13](#)
- [Directory Listing Pane, page 7-14](#)
- [Closing the View Editor Window, page 7-14](#)

Related Topics:

- [Choosing a View, page 7-14](#)
- [Chapter 10, “Viewing Network Topology.”](#)

View Editor Window Menu

The menu on the View Editor window contains:

Menu Command	Description
File > Load DEFAULT View	Loads the DEFAULT view, which is the view into which the MWTM places all discovered objects when discovering the network. The DEFAULT view is stored on the MWTM server, where all MWTM clients share the view; but cannot modify it.
File > Load (Ctrl-L)	Loads an already existing view. If you have already saved a view and you want to change it, choose the File > Load menu option. The MWTM prompts you for the name of the view you want to load: • Select the name of the view, or accept the default view name, then click OK to load the view. • Click Cancel to close the prompt window without loading a view.
File > Save (Ctrl-S)	Saves the current view. If you have: • Not already saved the current view, opens the Save File Dialog: View List, which you use to enter or select a filename under which to save the current view. • Already saved the current view, saves the view to that filename. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.

Menu Command	Description
File > Save As	Opens the Save File Dialog: View List, which you use to save changes you made to the chosen view with a new name, or overwrite an existing seed file. The view is updated immediately in the MWTM client. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
File > Close (Ctrl-W)	Closes the View Editor window. If you have modified the view, the MWTM asks if you want to save your changes. Click: • Yes to save your changes to the current view. • No to keep the current view as-is, without applying any changes. The MWTM closes the View Editor window. • Cancel to close the prompt window and return to the View Editor window without applying any changes to the current view.
Edit > Create Subview (Ctrl-N)	Creates a new subview for the chosen view or subview. Enter a name for the new subview.
Edit > Rename View (Ctrl-R)	Renames the chosen view. The new name can be from 1 to 30 characters, and can contain any letters, numbers, or special characters.
Edit > Include In View (Ctrl-I)	Includes the chosen object in the view.
Edit > Exclude From View (Alt-X)	Excludes the chosen object from the view. The MWTM also excludes the object and associated objects from the topology map. If you exclude all of the objects associated with a node, the node is excluded, too.
Edit > Delete View (Ctrl-D)	Deletes the chosen view.
Help > Topics (F1)	Shows the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Shows online help for the current window.
Help > About (F3)	Shows build date, version, SSL support, and copyright information about the MWTM application.

Objects In Current View

The navigation tree in the left pane of the View Editor window lists nodes that the current view contains.

To see the objects that are associated with a node, and that are in the current view, click the turner  beside the node.

To exclude any of these objects from the current view, select them in the navigation tree, then choose **Edit > Exclude From View** from the View Editor window to move them to the Excluded From View pane of the View Editor window.

**Note**

If you are using an MWTM client with the DEFAULT view set, the MWTM automatically adds all newly discovered objects to the navigation tree as soon as they are discovered.

If you delete an object, the MWTM removes it from the navigation tree. If the MWTM then discovers the object, the MWTM places it in the New on the Network pane. To see this object again in your current view, you must move it into the navigation tree using Edit > Include In View from the View Editor window.

The navigation tree in the View Editor window provides these right-click menus:

- [Right-Click Menu for a View, page 7-11](#)
- [Right-Click Menu for a Subview, page 7-11](#)
- [Right-Click Menu for an Object, page 7-11](#)

Right-Click Menu for a View

The right-click menu for a view in the navigation tree of the View Editor window provides these options:

Menu Command	Description
Create Subview	Creates a new subview for the chosen view. Enter a name for the new subview.
Rename View	Renames the chosen view. The new name can be from 1 to 30 characters, and can contain any letters, numbers, or special characters.

Right-Click Menu for a Subview

The right-click menu for a subview in the navigation tree of the View Editor window contains:

Menu Command	Description
Create Subview	Creates a new subview for the chosen subview. Enter a name for the new subview.
Rename View	Renames the chosen subview. The new name can be from 1 to 30 characters, and can contain any letters, numbers, or special characters.
Delete From View	Deletes the chosen subview from the view or subview.
Export View	Opens the Save File Dialog: View List dialog box, which you use to save the subview as a unique view.

Right-Click Menu for an Object

The right-click menu for an object in the navigation tree of the View Editor window provides this option:

Menu Command	Description
Exclude From View	Excludes the chosen object, and any lower-level associated objects, from the view or subview. This action also excludes the object from the topology map.

Excluded from View Pane

The Excluded from View pane lists the objects that have been excluded from the current view. To add these objects to the current view, select them in the Excluded from View pane, then choose **Edit > Include In View** from the MWTM main menu to move them to the navigation tree of the View Editor window.

The Excluded from View pane provides this right-click option for an object:

Menu Command	Description
Include In View	Includes the chosen object, and any lower-level associated objects, in the chosen view or subview.

New on the Network Pane

The New on the Network pane shows newly discovered objects, based on these criteria. If you are using an MWTM client with:

- The DEFAULT view set, this table never contains any objects. In the DEFAULT view, the MWTM adds all newly discovered objects to the navigation tree in the View Editor window as soon as they are discovered.
- A custom view set, this table contains all objects discovered since the View Editor window was opened in this session that have *not* been excluded in the Excluded from View pane or that are not in the current view.

When the MWTM discovers one or more new objects in the network, the MWTM also:

- Broadcasts the discovery of the new objects to all MWTM clients.
- Shows a **New** icon in the bottom of most MWTM windows. Clicking the **New** icon in the topology window opens the New Objects pane in the left pane. Clicking the **New** icon in any other window opens the Edit View tab of the View Editor window.
- Adds graphical elements for the newly discovered objects to the New Objects pane in the left pane of the topology window. For more information, see [Printing the Topology Map, page 10-18](#).

To add a newly discovered object to the current view, select one or more objects in the New on the Network pane, then choose **Edit > Include In View** from the MWTM main menu to move them to the navigation tree in the View Editor window.

To exclude a newly discovered object from the current view, select one or more objects in the New on the Network pane, then choose **Edit > Exclude From View** from the MWTM main menu to move them to the Excluded From View pane of the View Editor window.

The New on the Network pane provides these right-click options for an object:

Menu Command	Description
Include In View	Includes the chosen object, and any lower-level associated objects, in the chosen view or subview.
Exclude From View	Excludes the chosen object, and any lower-level associated objects, from the view or subview. The MWTM also removes the object from the topology map.

Views List Pane

The Views List pane is under the Import Views tab of the View Editor window. The Views List pane lists all views that are currently defined on this MWTM client. If you have no views defined, this list will be empty.

You can resize each column, or sort the table based on the information in one of the columns. By default, this table is sorted by Name, and the MWTM shows all of the columns in the Views List pane.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Views List pane contains these columns:

Column	Description
Type	Indicates whether the chosen name is a directory or a file.
Name	Name of the view.
Last Modified	Date and time the view was last modified.
Size (bytes)	Size of the view in bytes.

The Views List pane provides these right-click menu option for views:

Menu Command	Description
Import View	Copies the chosen view into the view or subview that is currently chosen in the navigation tree of the View Editor window.
Delete View	Deletes the chosen folder, view, or subview. (You can delete a folder only if it contains no views or subviews.)

The Views List pane provides these right-click menu option for folders:

Menu Command	Description
Open View	Opens the chosen folder, displaying views contained in the folder in the Views List pane.

View Data Pane

The View Data pane lists all subviews and objects that are in the view that is chosen in the Views List pane. If you have not saved a view yet, and there are no views in the Views List pane, this pane does not appear.

The View Data pane provides these right-click menu option for views and subviews:

Menu Command	Description
Import View	Copies the chosen view or subview into the view or subview that is currently chosen in the navigation tree of the View Editor window.

Directory Listing Pane

The Directory Listing pane lists all subfolders that are in the folder that is chosen in the Views List pane. If the Views List pane contains no views, or if a folder (not a file) exists in the Views List pane, the Directory Listing pane appears. If the Views List pane contains only files, the Directory Listing pane does not appear.

To see the Directory Listing pane, select a folder in the Views List pane.

Closing the View Editor Window

To close the View Editor window at any time, click **File > Close**. If you have modified the view, the MWTM asks if you want to apply the changes before leaving the window. Click:

- **Yes** to apply the changes to the current view. The MWTM applies the changes to all MWTM windows immediately. The MWTM then asks if you want to make this the default view. Click:
 - **Yes** to make this view the new default view. In the future, when this client is started, this will be the default view.
 - **No** to retain your old default view.

The MWTM closes the View Editor window.

- **No** to keep the current view unchanged, without applying any changes. The MWTM closes the View Editor window.
- **Cancel** to close the prompt window and return to the View Editor window without applying any changes to the current view.

If you are working in a custom view (that is, not in the DEFAULT view) and you exit the MWTM client, the MWTM automatically saves any changes you made to the view.

Choosing a View

If you are performing an action and have multiple views from which to choose, the Choose a View dialog box appears. Use it to choose the view you wish to apply.

The Choose a View dialog box contains:

Field or Button	Description
View List	Shows a list of views available for this action.
OK	Confirms the view you have chosen.
Cancel	Cancels the dialog without choosing a view.
Help	Shows help for this dialog box.

Loading the DEFAULT View

To load the DEFAULT network view, choose **File > Load DEFAULT View** from the MWTM main menu. You might be prompted to save the view in which you currently are. Once you have chosen whether to save your current view, the MWTM loads the DEFAULT view.

**Note**

Any custom views are saved in the View Editor window (Import Views tab) under the Edit > Views option in the MWTM main window.

Loading a Client-Specific View

You use the MWTM to load a specific view, change the list of views, and select one view to be loaded automatically when the associated preferences file is loaded.

To load a client-specific network view, choose **Edit > Views** from the MWTM main menu. The View Editor window appears. Then choose **File > Load** from the View Editor window menu. The MWTM shows the Load File Dialog: View List dialog box.

The Load File Dialog: View List contains:

Field or Button	Description
Type	Icon indicating whether the item in the table is a file or a folder.
Name	Name of the view file or folder.
Last Modified	Date and time the view file or folder was last modified.
Size (bytes)	Size of the view file or folder, in bytes.
Make this my preferred start option	Specifies whether the chosen view should be loaded automatically whenever the associated preferences file is loaded. To load the: - Chosen view, select the view, then check this check box. - Last-used view, uncheck the check box. This is the default setting.
Number of Files (visible in bottom left corner)	Total number of view files and folders.
OK	Loads the chosen view, saves any changes you made to the list of views, closes the dialog box, and returns to the View Editor window. To load a view, double-click it in the list, select it in the list and click OK, or enter the name of the view and click OK. Note If the network elements belonging to a client-specific view have been removed from the network, a message appears when you load the view. The message warns you that the network elements have been removed from the view. To prevent the warning from being issued the next time you load the view, save the view using the same name (File > Save from the View Editor window).
Delete	Deletes the chosen file from the view list. The MWTM issues an informational message containing the name and location of the deleted file.

Field or Button	Description
Cancel	Closes the dialog box without loading a view or saving any changes to the view list.
Help	Shows online help for the dialog box.

Ignoring a View

You can instruct the MWTM to ignore a view when it aggregates and shows network data. Setting views to Ignored prevents known problems in the views from affecting MWTM displays for associated objects. In effect, you are preventing a known problem from distracting you from other, more urgent network problems.

For example, you can set a view to Ignored before shutting down objects in the view for maintenance.



Note

If you set a view to Ignored, the view is ignored for only the current MWTM client.

Also, if you set a view to Ignored, make a note of the change, and do not forget to reset the view when the problem is corrected or the maintenance is complete.

You cannot ignore the DEFAULT view.

To set a view to Ignored, check the **Ignored** check box in the View window for the view you want the MWTM to ignore.

Viewing Ignored Views

To display all views that are Ignored, display the View window and click the Ignored column heading. The MWTM shows all ignored views at the top of the table.



CHAPTER 8

Understanding Detailed Object Functions

You can use the Cisco Mobile Wireless Transport Manager (MWTM) to view detailed information about any discovered MWTM object, including its associated objects, status, notes, alarms and events, and so on.

To display detailed information for an object:

-
- Step 1** In the navigation tree of the MWTM main window, click the turner  beside a view.
- Step 2** Click a node. The Details tab appears in the content pane (see [Viewing Details, page 8-12](#)).
-

This chapter contains:

- [Viewing the Right-Click Menu for an Object, page 8-3](#)
- [Deploying a File Associated with an ITP Node or Signaling Point, page 8-9](#)
- [Viewing Management Interfaces and Physical Folders, page 8-9](#)
- [Viewing Status Contributors, page 8-10](#)
- [Viewing Details, page 8-12](#)
- [Viewing Troubleshooting, page 8-43](#)
- [Viewing Alarms and Recent Events, page 8-45](#)
- [Using Provisioning, page 8-46](#)
- [Editing SNMP IP Addresses for a Node, page 8-51](#)
- [Polling a Node, page 8-53](#)
- [Allowing and Disallowing Trap Processing for a Node, page 8-56](#)
- [Viewing Real-Time Data, page 8-56](#)
- [Viewing ITP Linkset Access Lists, page 8-123](#)
- [Viewing Data Specific for ITP Signaling Points, page 8-123](#)
- [Viewing RAN Shorthauls, page 8-140](#)
- [Creating Virtual RAN Backhauls, page 8-140](#)



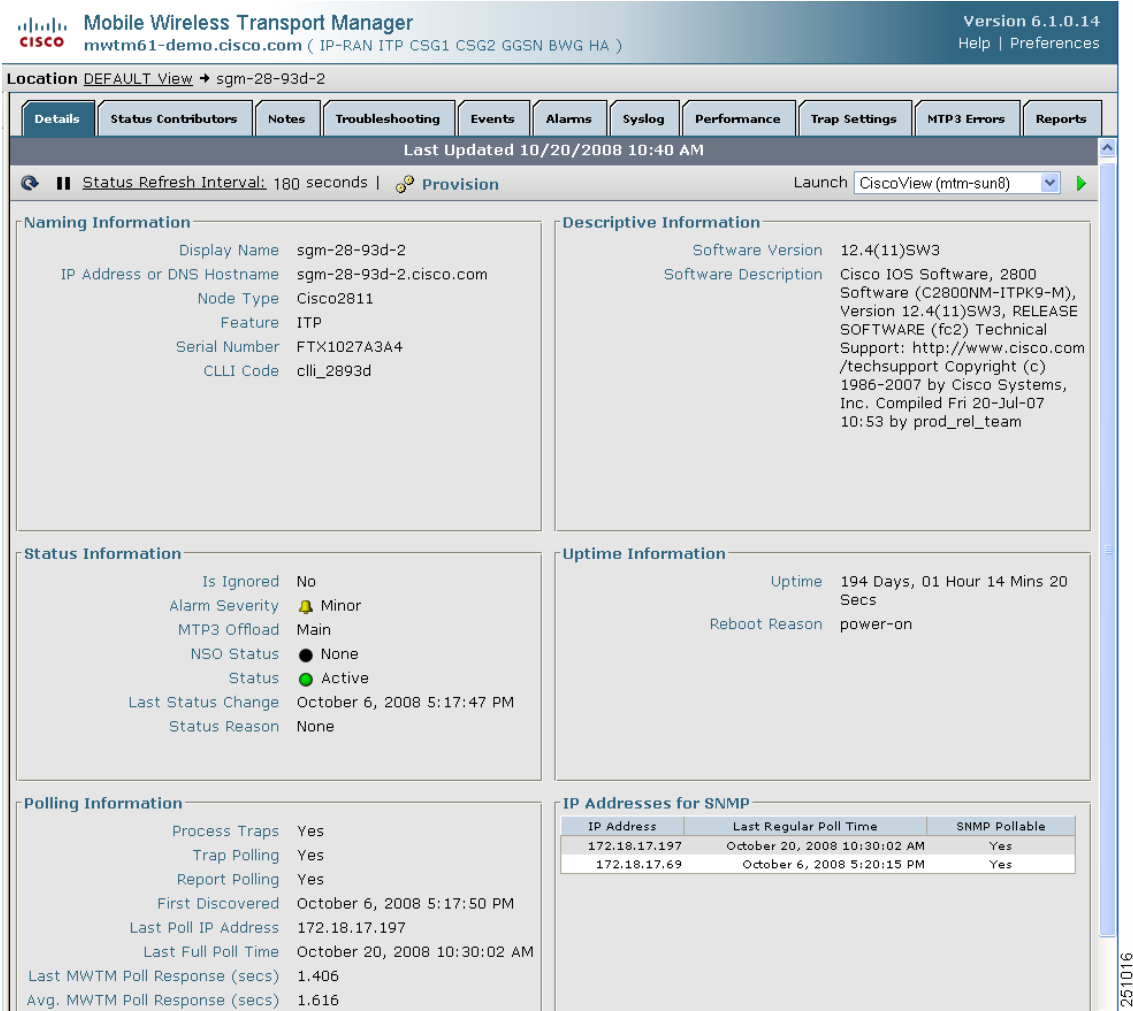
Note

For details on viewing notes, see [Viewing Notes, page 6-39](#).

The MWTM displays detailed tabular information in the content area for the chosen object. Tabs will vary depending on the chosen object.

For example, if you choose an ITP node, the ITP Node table for that node displays as shown in Figure 8-1.

Figure 8-1 Example—IPT Node Tabs



Note

The tabs automatically reflect updates for the object from the MWTM server.

Viewing the Right-Click Menu for an Object

Right-clicking on any object in an MWTM view, summary list, or topology map provides you with numerous menu options.

Example:

To see the right-click menu for a node, select a node in the navigation tree and right-click the mouse button.

These right-click menu options might be available on a given MWTM object:

Menu Command	Description
Show In New Window	Opens the Details window for the chosen object in a new window.
Edit > Properties	Opens the Edit Properties dialog box for the chosen node or ITP signaling point. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
Edit > Notes	Opens the Edit Notes dialog box for the chosen object. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
Edit > SNMP IP Addresses	Opens the Edit SNMP IP Addresses dialog box for the chosen node. This option is dimmed if the chosen node has no associated SNMP IP addresses. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Edit > Route Table (ITP signaling points only)	Opens the Route Table dialog box, using a route table from the signaling point. This option is not available if the node associated with chosen signaling point is in Unknown or Unmanaged status. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Clear Event Icon	Deletes the event icon  from MWTM displays for the chosen object, for this MWTM client only. The MWTM does not delete the actual events, but deletes only the event icon for the chosen object for this MWTM client. This option is dimmed if the chosen object has no associated event icon.

Menu Command	Description
Delete	Deletes the currently chosen object from the MWTM database. The MWTM displays the Confirm Deletion dialog box. To: - Delete the chosen object, click Yes. The MWTM deletes the object from the MWTM database and closes the Confirm Deletion dialog box. - Retain the chosen object, click No. The MWTM retains the object in the MWTM database and closes the Confirm Deletion dialog box. Note (ITP only) If you delete all linksets to an Unmanaged node, the MWTM does not automatically delete the node. Instead, you must manually delete the node. See Deleting Objects, page 6-40 for more information. - Prevent the MWTM from displaying the Confirm Deletion dialog box, check the Do not show this again check box. Note If you check the Do not show this again check box, and later you decide you want the MWTM to begin displaying the Confirm Deletion dialog box again, you must check the Confirm Deletions check box in the General GUI settings in the Preferences window. For more information, see the description of the Confirm Deletions check box in Startup/Exit Settings, page 5-4. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Go to > <i>Object</i>	Navigates to the parent or peer (if applicable) window(s) for the chosen object.
Back > <i>List of windows</i>	Navigates back to a window viewed in this session. The MWTM maintains a list of up to 10 Back windows.
Forward > <i>List of windows</i>	Navigates forward to a window viewed in this session. The MWTM maintains a list of up to 10 Forward windows.
Show Peer (only for RAN Backhauls and RAN Shorthauls)	Shows the peer of the RAN backhaul or shorthaul that you select in the right pane.
View > Status Contributors	Displays the Status Contributors pane for the chosen object. Objects in this pane contribute to the status of the chosen object.
View > Details	Displays the Details pane for the chosen object.
View > Notes	Displays the Notes pane for the chosen object. If no notes are associated with the chosen object, this option is dimmed.

Menu Command	Description
View > Troubleshooting	Displays the Troubleshooting pane for the chosen object. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.
View > Recent Events	Displays the Recent Events pane for the chosen object and any associated network objects.
View > Alarms	Displays the Alarms pane for the chosen view.
View > Real-Time Data and Charts	Displays the MWTM Real-Time Statistics window for the chosen object. This option is not available if the object has no real-time charts or if the object status is Unknown or Unmanaged.
View > Center in Topo	Opens the topology window and displays the object in the center of the topology map.
View > Advanced Details (Web)	Opens the MWTM web client to display the Statistics tab for the selected object. This option appears only for those objects that have advanced details.
Archived Events > Status Changes	Displays the archived status changes in a web browser.
Archived Events > SNMP Traps	Displays the archived SNMP traps in a web browser.
Archived Events > Status Changes and SNMP Traps	Displays both the archived status changes and archived SNMP traps in a web browser.
Ignore	Ignores the chosen object at the next polling cycle. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
Unignore	Stops ignoring the chosen object at the next polling cycle. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
Performance History (RAN-O backhauls and shorthauls only)	Displays historical performance charts for the chosen RAN-O backhaul or shorthaul in a web browser.
Error History (RAN-O backhauls and shorthauls only)	Displays historical error charts for the chosen RAN-O backhaul or shorthaul in a web browser.
Create Virtual RAN Backhaul (RAN-O backhauls only)	Opens the Virtual RAN Backhaul Editor. For details, see Creating Virtual RAN Backhauls, page 8-140 .
Drill-Down > <i>List of windows</i>	Opens a specific tab for the chosen object. Tabs listed start a poller. This option is not available if the node is in Unknown or Unmanaged status.

Menu Command	Description
Latest Reports	Opens the latest reports for the object in a Web browser. For details on reports, see Chapter 12, “Managing Reports.” This option is not available if the node is in Unknown or Unmanaged status.
Provision	Opens the web interface to the Provision tab of the chosen object (see Using the Provisioning Wizard, page 8-50).
Launch	Use it to launch: • CiscoView • Device Center Note You must first integrate these applications with the MWTM. See Integrating the MWTM with CiscoWorks, page 5-39.

Menu Command	Description
These menu options are available on nodes or ITP signaling points:	
Node > Home Page	Displays the home page of the node in a new web browser window. This option does not appear in the right-click menu for Cisco Optical Networking System (ONS) nodes or nodes that are unknown. For a Cisco Data for Telecommunications (CDT) node, this option launches the CDT login web page.
Node > Launch CTC (ONS nodes only)	Launches the Cisco Transport Controller (CTC) for managing ONS nodes. For more information about using the CTC, refer to the <i>CTC Launcher Application Guide</i> (http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_configuration_guide09186a008051ea52.html). This option appears only for ONS nodes.
Node > Connect To	Links to the node. This option is dimmed if the chosen node has no IP addresses. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.
Poll Node > Normal Poll	Polls all chosen nodes or ITP signaling points, retaining all currently known objects. Normal Poll retains all objects associated with polled nodes or signaling points, even objects that have been deleted and are, therefore, in Unknown status. This option is dimmed if the chosen node has no IP addresses. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.
Poll Node > Clean Poll	Polls all chosen nodes or ITP signaling points and removes any Unknown network objects after the completion of the poll. Clean Poll removes all network objects from the node or signaling point at the completion of the poll. This option is dimmed if the chosen node has no IP addresses. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

Menu Command	Description
Allow Trap Processing	Enables the MWTM to process traps from the chosen node. This is the default setting. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 4) and higher.
Disallow Trap Processing	Prevents the MWTM from processing traps from the chosen node. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 4) and higher.
Unmanage	Labels the chosen node or signaling point Unmanaged. Note If you change a node to the Unmanaged status, the MWTM removes adjacent legacy nodes from the topology map. You cannot label a node or signaling point Unmanaged if it has a Node Type of Unknown. If you select a node or signaling point with a Node Type of Unknown, then this menu option is dimmed and cannot be chosen. This option is dimmed if the chosen node has no IP addresses. Events for unmanaged objects will continue to appear in the Events window. To suppress events for unmanaged objects, set this option using an event filter (Setting an Alarm or Event Filter, page 9-18). If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Manage	Removes the Unmanaged status from the chosen node or signaling point. Note If you change a node to the Managed status, the MWTM adds adjacent legacy nodes back to the topology map. You cannot remove the Unmanaged status from a node with a Node Type of Unknown. If you select a node with a Node Type of Unknown, then this menu option is dimmed. This option is dimmed if the chosen node has no IP addresses. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

Menu Command	Description
Exclude from View	Excludes the chosen node or signaling point from the current view. See Creating a New View, page 7-8 for more information about excluding objects. The MWTM removes excluded objects and their associated objects from the topology map (see Excluded Objects Tab, page 10-10).
Deploy <i>Object</i> > From Archive (ITP only)	Launches the Deployment Wizard for the chosen node or ITP signaling point. See Deploying a File Associated with an ITP Node or Signaling Point, page 8-9 for more information about deploying to nodes or ITP signaling points.
Deploy <i>Object</i> > From File (ITP only)	Launches the Deployment Wizard for the chosen node or ITP signaling point. See Deploying a File Associated with an ITP Node or Signaling Point, page 8-9 for more information about deploying to nodes or ITP signaling points.

Deploying a File Associated with an ITP Node or Signaling Point

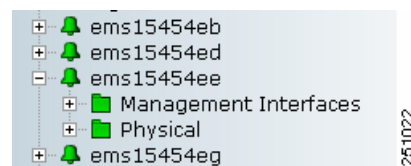
You use the MWTM to deploy a GTT file or route table file associated with an ITP node or signaling point. To do so, right-click the ITP node or signaling point in a window, then choose **Deploy Object > From Archive** or **From File** in the right-click menu. The MWTM launches the Deployment Wizard for the chosen ITP node or signaling point. See [Deploying a Route Table File, page 13-13](#) and [Deploying a GTT File, page 14-37](#) for more information.

Viewing Management Interfaces and Physical Folders

ITP, IPRAN, and mSEF nodes can contain:

- **Management Interfaces**—A folder that contains a list of interfaces that the MWTM uses to manage the node.
- **Physical**—A folder that contains a list of the physical interfaces and ONS cards that belong to the node. Slot numbers precede ONS card objects (for example, *15 - RAN_SVC* or *02 - E1-42*).

Figure 8-2 Management Interfaces and Physical Folders



All objects in the Physical folder are ignored *unless* they also appear outside of the Physical folder. The status of Physical folder-only objects do not contribute to the status of the parent node. These objects also do not appear in the Active Alarms list, but they do appear in the Event History. You can un-ignore the Physical folder, then re-ignore the objects you do not want to monitor. For more information, see [Why are objects in the Physical folder ignored?, page C-8](#)).

Viewing Status Contributors

The Status Contributors section displays information about conditions that contribute to the overall status of the chosen object. To view the Status Contributors section, select an object in the navigation tree and click the Status Contributors tab in the right pane.

The content pane lists all objects contributing to the status of the object you have chosen in the navigation tree. A tooltip in the content pane lists the fully qualified domain name (FQDN) for the object.

To see which object types pertain to the Status Contributors tab, see [Appendix A, “Client Object Map Reference.”](#) If the object does not have any associated objects, the Status Contributors tab will not appear.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns except Internal ID.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24.](#)

The Status Contributors table contains:

Column	Description
Internal ID	Internal ID of the object. The internal ID is a unique ID for every object, assigned by the MWTM for its own internal use. It can also be useful when the TAC is debugging problems.
Name	Name of the object.
Object Type	Type of network object.
Ignored	Indicates whether the object should be included when aggregating and displaying MWTM status information: • Uncheck the check box to include the object. This is the default setting. • Check the check box to exclude the object. This field can be edited by users with authentication level Power User (level 2) and higher.
Notes	Indicates whether a note is associated with the object.
Events	Indicates whether the object has an associated recent event. (Even if the server purges all of the events associated with the object, the MWTM continues to display the event icon in this field.) To: • Delete the event icon (orange triangle) from MWTM displays for a specific object, select the object and click the icon. • Delete the event icon from MWTM displays for all objects, choose Edit > Clear All Events from the MWTM main menu. Note During Discovery, the MWTM might flag objects with an event icon. If the event icons are too distracting, use the Edit > Clear All Events menu option to remove them.
Last Status Change	Date and time that the status of the object last changed.
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”

Column	Description
Status	Current status of the object. Possible values are:  Active  Blocked  Discovering  Down  Failed  Inactive  Inhibited  InhibitLoc  InhibitRem  None  Not Present

Column	Description
Status (continued)	 Old Unmanaged  Pending  Polling  Shutdown  Unavailable  Unknown  Unmanaged  Waiting  Warning For detailed definitions of each status, see Status Definitions for Signaling Gateway Mated Pairs, page E-7.
Status Reason	Reason for the current status of the object. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If: - You installed the MWTM in the default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOs/gm/apache/share/htdocs/eventHelp</i> directory. - You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The MWTM lists status reasons in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

Viewing Details

The Details section displays information such as naming and status details for the chosen object.

To view the Details section, select a view in the navigation tree, select an object, then click the Details tab in the right pane.



Note

If the chosen object is a link, linkset, signaling gateway-mated pair, RAN-O backhaul or shorthaul, the Details tab displays both peers of the chosen object in adjacent panes for easy comparison.

The Details tab contains these sections (in alphabetical order):

Section	Applicable Object(s)	Applicable Network Type(s)
Address Information	Interfaces	All networks
Advanced Details (Web)	Nodes	BWG, CSG2, HA, and GGSNs on card
Association Information	Application Servers	ITP only
Bandwidth Information	Backhauls	RAN-O only
Capability Point Code	Signaling Points	ITP only
Description	Linksets, Signaling Points	
Descriptive Information	Cards, Nodes	All networks
General Information	Application Servers, Application Server Process Associations, Interfaces, Linksets, Shorthauls	
Interface Information	Links, Signaling Gateway Mated Pairs	ITP only
IP Addresses for SNMP or IP Addresses Not for SNMP	Nodes	All networks
Links Information	Linksets	ITP only
Local IP Address Information	Application Server Processes, Application Server Process Associations, Links, Signaling Gateway Mated Pairs	
Naming Information	All objects	All networks
Point Code	Signaling Points	ITP only
Polling Information	Nodes	All networks
Protection Information	Cards, ONS Nodes	RAN-O only
QoS Information	Signaling Points	ITP only
RAN Information	Interfaces, Shorthauls	RAN-O only
Remote IP Address Information	Application Server Process Associations, Links, Signaling Gateway Mated Pairs	ITP only
Status Information	All objects	All networks
Threshold Information (RAN-O Only)	Backhauls, Nodes	RAN-O only
Uptime Information	Nodes	All networks

**Tip**

If the pair of a link, linkset, or signaling gateway-mated pair is Unknown, and if the peer of a backhaul or shorthaul is Unknown, `Unknown` appears for the pair or peer fields in the Details tab.

Address Information

The Address Information section for interfaces contains:

Field	Description
IP Address	List of IP addresses that are assigned to the interface.

Advanced Details (Web)

The Advanced Details (Web) link appears in the MWTM client and launches the MWTM web interface to display the Statistics tab for the selected node. The Advanced Details (Web) link enables you to access advanced statistics that are available only for these nodes:

- CSG2 (see [Displaying CSG2 Real-Time Statistics, page 11-44](#))
- BWG (see [Displaying BWG Real-Time Statistics, page 11-49](#))
- HA (see [Displaying HA Real-Time Statistics, page 11-62](#))
- GGSN on a SAMI card (see [Displaying GGSN Real-Time Statistics, page 11-65](#))

Association Information

The Association Information section for ITP application servers contains:

Field	Description
Number of ASPAs	Number of application server process associations that are associated with this application server.
Number of Active ASPAs	Number of active application server process associations that are associated with this application server.

Bandwidth Information

The Bandwidth Information section for RAN-O backhauls (and virtual backhauls) contains:

Field	Description
User Send Bandwidth (bits/sec) User Receive Bandwidth (bits/sec)	Bandwidth that the user specifies for the backhaul. Send and receive bandwidth values will be different if the interface is asymmetrical. By default, the user bandwidth is the same as the system bandwidth. Note When you change the User Bandwidth (see Editing Properties for a RAN-O Backhaul, page 6-36), you are changing the scale of the Y axis of the backhaul real-time chart in the Performance tab (see Viewing Backhaul Performance Data, page 8-111). The X and Y values of the data do not change. The threshold ranges resize because they are percentages of User Bandwidth.
System Send Bandwidth (bits/sec) System Receive Bandwidth (bits/sec)	Bandwidth that the system specifies (as defined on the node) for the backhaul. Send and receive bandwidth values will be different if the interface is asymmetrical. You cannot edit this field.

Capability Point Code

The Capability Point Code section for ITP signaling points contains:

Column	Description
Point Code	Capability point code of the signaling point.
Variant	SS7 protocol variant. Valid variants are: • ANSI • China • ITU • NTT • TTC

Column	Description
Network Indicator	Determines the type of call. Valid values are: • National—National-bound call. The MWTM routes national calls through the national network. • NationalSpare—National-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates networks. • International—International-bound call. The MWTM forwards international-bound calls to an STP pair that acts as an international gateway. • InternationalSpare—International-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates networks.
Network Name	Name of the network associated with the signaling point.

Description

The Description section contains a description of the ITP signaling point or linkset. If the signaling point or linkset has no description, this section is blank. If the linkset is unknown, Unknown appears in the Description section.

Descriptive Information

The Descriptive Information section for nodes and ONS cards contains:

Field	Description
Software Description	Comprehensive information about the software that is installed on the node.
Software Version	Version of software (for example, the ONS package or IOS version) that is installed on the node.
Description	Full description of the ONS card (for example, RAN_SVC_LINE_CARD).
Hardware Version	Version of the hardware of the ONS card (for example, VID=000, HwRev=29).
Firmware Version	Version of the firmware on the ONS card, if applicable (for example, 12.2(24)St).

General Information

The General Information section applies to these objects:

- [Interfaces, page 8-17](#)
- [ITP Application Servers, page 8-17](#)
- [ITP Linksets, page 8-18](#)

Interfaces

The General Information section for interfaces contains:

Field	Description
Maximum Packet Size	Maximum packet size on the interface in bytes.
Send Speed (bits/sec)	Interface send speed in bits per second.
Receive Speed (bits/sec)	Interface receive speed in bits per second.

ITP Application Servers

The General Information section for ITP application servers contains:

Field	Description
Protocol	Protocol associated with the application server. Possible values are: • M3UA—MTP3-User Adaptation. • SUA—SCCP-User Adaptation.
QoS	Quality of service (QoS) class of the application server.
Routing Key	Routing key associated with the application server. The routing key is the value that determines the routing decisions that the application server makes.
Traffic Mode	Method by which the application server forwards requests to its active application server processes. Possible values are: • overRide—One application server process takes over all traffic for the application server, possibly overriding any currently active application server process in the application server. • broadcast—Every active application server process receives the same message. • loadBind—Each application server process shares in the traffic distribution with every other currently active application server process, based on application server process bindings. • loadRndRobin—Each application server process shares in the traffic distribution with every other currently active application server process, using a round-robin algorithm. • undefined—The traffic mode is not defined. The first application server process that becomes active defines the traffic mode.

ITP Linksets

The General Information section for ITP linksets contains:

Field	Description
Linkset Type	Type of linkset, which the MWTM determines by examining the links defined in the linkset. Possible linkset types are: • HSL—The links in this linkset use the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol. • SCTPIP—The links in this linkset use the Stream Control Transmission Protocol (SCTP) IP transport protocol. • Serial—The links in this linkset use the serial SS7 signaling protocol. • Mixed—The links in this linkset are of two or more types. (This configuration is not recommended.) • Virtual—The links in this linkset are virtual links, which connect signaling point instances running on the same node. The MWTM does not poll virtual linksets, nor does it display real-time data or accounting statistics for virtual linksets. Note Prior to IOS release 12.2(23)SW1, the user manually created virtual linksets on multi-instance nodes. In and after that release, the system automatically creates virtual linksets. • Other—No links have been defined for this linkset.
Inbound ACL	Inbound IP access control list (ACL) number for the linkset. If no inbound ACL exists for the linkset, this field displays 0. If the linkset is a Virtual linkset, this field displays N/A.
Outbound ACL	Outbound ACL number for the linkset. If no outbound ACL exists for the linkset, this field displays 0. If the linkset is a Virtual linkset, this field displays N/A.

Interface Information

The Interface Information section for ITP links and application server process associations contains:

Field	Description
Interface Name	(HSL, Serial, and Virtual links only) Name of the interface.
Interface Index	(HSL, Serial, and Virtual links only) Index into the SNMP interface table.
QoS	(SCTP links only) Quality of service (QoS) class of the link.
Configured Local Port	(SCTP links only) Local port for which the link was configured.
Local Port	(SCTP links only) If the link is active, local port that the link is currently using. If the link is not active, 0 appears.

Field	Description
Configured Remote Port	(SCTP links only) Remote port for which the link was configured.
Actual Remote Port	(SCTP links only) If the link is active, remote port that the link is currently using. If the link is not active, 0 appears.
Protocol	Protocol associated with the application server process association. Possible values are: M3UA—MTP3-User Adaptation. SUA—SCCP-User Adaptation.

IP Addresses for SNMP

The IP Addresses for SNMP section for nodes contains:

Field	Description
IP Address	IP addresses associated with this node, including the primary SNMP address and all backup IP addresses, that are intended for SNMP.
Last Regular Poll Time	Date and time of the last full poll of the node. If the IP address has never been polled, the MWTM displays the description <code>Never Polled</code> .
SNMP Pollable	Whether or not the IP address is used for SNMP polling.

If there are no IP addresses defined for the node that are intended for SNMP, this field displays the description:

`There are no other IP addresses defined for this node.`

IP Addresses Not for SNMP

The IP Addresses Not for SNMP section for nodes contains:

Field	Description
IP Address	IP addresses associated with this node that are <i>not</i> intended for SNMP.

If no IP addresses are defined for the node that are not intended for SNMP, this field displays the description:

`There are no other IP addresses defined for this node.`

Links Information

The Links Information section for ITP linksets contains:

Field	Description
Links	Total number of links in the linkset.
Active Links	Number of links in the linkset that are Active.
Congested Links	Number of links in the linkset that are Congested.

Local IP Address Information

The Local IP Address Information section for ITP application server processes, application server process associations, SCTP links, and signaling gateway mated pairs contains:

Field	Description
IP Address	Local IP address that the object is using, or the primary IP address that is configured for the object, or both. The primary IP address is the first CS7 local IP address you configure in the node. For example, if you configure these IP addresses in the node: <pre>cs7 local-peer 4180 local-ip 128.3.0.77 local-ip 128.3.0.254</pre> then the MWTM uses 128.3.0.77 as the primary IP address. If someone deletes this IP address from the node configuration, or adds a new IP address to the beginning of the list, the MWTM detects the change and automatically updates this field to reflect the new primary IP address.
Interface Name	Name of the interface to which the IP address is assigned. If the object has no interface name, this field is blank.
Status	Current status of the IP address. Possible values are:  Active—The IP address is currently fully functional.  Inactive—The IP address is not currently functional.
Cfg	Indicates whether this local IP address was configured for the object. Possible values are: Yes—This is the configured local IP address, and the object is currently using it. (blank)—This is not the configured local IP address.
Actual	Indicates whether this local IP address is currently being used by the object. Possible values are: Yes—The object is currently using this IP address. (blank)—The object is not using this IP address.

Naming Information

The Naming Information section applies to these objects:

- [Nodes, page 8-21](#)
- [Cards, page 8-22](#)
- [Interfaces, page 8-22](#) (including RAN backhauls and shorthauls)
- [ITP Application Servers, page 8-23](#)
- [ITP Application Server Processes, page 8-23](#)
- [ITP Application Server Process Associations, page 8-23](#)
- [ITP Links, page 8-23](#)
- [ITP Linksets, page 8-24](#)
- [ITP Signaling Gateway-Mated Pairs, page 8-24](#)
- [ITP Signaling Points, page 8-24](#)

Nodes

The Naming Information section for nodes contains:

Field	Description
Display Name	Name of the node.
IP Address or DNS Hostname	IP address or DNS name of the node, as the MWTM discovered it. However, if you modified your preferences to identify nodes by their IP addresses, then this is method of node identification in this field. For more information, see Node Name Settings, page 5-5 .
Node Type	Type of node. See Nodes Table, page 6-5 , for a list of the available node types.
Feature	Primary function performed by the node type. See Nodes Table, page 6-5 , for a list of the available features.
Chassis Type (ONS only)	Description of the chassis hardware type (for example, ONS 15454 SDH ETSI). Note This field appears only for the ONS chassis.
Serial Number	Serial number of the node.
CLLI Code (ITP only)	COMMON LANGUAGE Location Identification Code for the node. A CLLI code is a standardized 11-character identifier that uniquely identifies the geographic location of the node. If the node has no CLLI code configured, this field is blank.
SNMP Access (RAN-O only)	Indicates the type of SNMP access: • In-band—Access is through the backhaul interface (cell site). • Out of band—Access is external to the backhaul interface (aggregation site). • Undefined—Access is not defined.
Location (RAN-O only)	The location of the SNMP settings, whether at the cell site (BSC) or the aggregation node site (BTS). ¹

Cards

The Naming Information section for ONS cards contains:

Field	Description
Name	Name of the card.
Card Type ¹	Type of card. Card types for ONS include: • TCC—Control • E1—Ethernet • STM1—Synchronous Transport Module • DS1—Digital Signal • OC3—Optical • XC—Cross-connect
Card Type (continued)	• RAN_SVC—RAN Service • ALM_PWR—Alarm and Power • CRFT_TMG—Craft Terminal • AICI—Alarm Interface Controller
Model Name	Model name of the card (for example, PartNum=800-26651-01).
Slot Number	Slot number of the card in the ONS chassis.
Serial Number	Serial number of the card.

1. See the *Cisco ONS 15454 Product Overview* for information about ONS cards:
<http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/45431po.htm>

Interfaces

The Naming Information section for interfaces (which includes RAN backhaul and shorthaul interfaces) contains:

Field	Description
Name	Name of the interface.
Node	Name of the node to which the interface belongs.
Physical Address	Physical address of the interface.
Interface Index	Interface index number.
Interface Type	Interface type.
RAN Connection To	RAN connection that is associated with the interface. Note Not visible for RAN backhauls.
Virtual RAN Backhaul	Whether the RAN backhaul is a virtual backhaul. For more information about virtual RAN backhauls, see Creating Virtual RAN Backhauls , page 8-140. Note Visible only for RAN backhauls.

ITP Application Servers

The Naming Information section for ITP application servers contains:

Field	Description
Name	Name of the application server.
Node	Name of the node associated with the application server.
Signaling Point	Name of the signaling point associated with the application server.

ITP Application Server Processes

The Naming Information section for ITP application server processes contains:

Field	Description
Name	Name of the application server process.
Node	Name of the node associated with the application server process.
Local Port	Local port number that the application server process is currently using.

ITP Application Server Process Associations

The Naming Information section for ITP application server process associations contains:

Field	Description
Name	Name of the application server process association.
Node	Name of the node associated with the application server process association.
Signaling Point	Name of the signaling point associated with the application server process association.
Application Server	Name of the application server associated with the application server process association.
Application Server Process	Name of the application server process associated with the application server process association.

ITP Links

The Naming Information section for ITP links contains:

Field	Description
Node	Name of the node associated with the link.
Signaling Point	Name of the signaling point associated with the link.
Linkset	Name of the linkset associated with the link.

Field	Description
SLC	Signaling link code (SLC) ID for the link.
Type	Type of link. Possible link types are: • HSL—The link uses the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol. • SCTPIP—The link uses the Stream Control Transmission Protocol (SCTP) IP transport protocol. • Serial—The link uses the serial SS7 signaling protocol. • Virtual—The link is a virtual link, which connects signaling point instances running on the same node. The MWTM does not poll virtual links, nor does it display real-time data or accounting statistics for virtual links.

ITP Linksets

The Naming Information section for ITP linksets contains:

Field	Description
Name	Name of the linkset.
Node	Node associated with the linkset.
Signaling Point	Signaling point associated with the linkset.
Local Point Code	Point code of the primary signaling point for the linkset.
Adj Point Code	Point code of the adjacent signaling point for the linkset.

ITP Signaling Gateway-Mated Pairs

The Naming Information section for ITP signaling gateway-mated pairs contains:

Field	Description
Name	Name of the signaling gateway-mated pair.
Node	Name of the node associated with the signaling gateway-mated pair.
Is Passive	Indicates whether the signaling gateway-mated pair can initiate the connection to the mate: • Yes—The signaling gateway-mated pair is passive, and cannot initiate the connection to the mate. • No—The signaling gateway-mated pair is not passive, and can initiate the connection to the mate.

ITP Signaling Points

The Naming Information section for ITP signaling points contains:

Column	Description
Name	Name of the signaling point.
Node	Name of the node associated with the signaling point.
Network Name	Name of the network associated with the signaling point.
Instance Number	Number of the instance associated with the signaling point.

Point Code

The Point Code section for ITP signaling points contains:

Column	Description
Point Code	Primary and secondary point codes of the signaling point.
Variant	SS7 protocol variant. Valid variants are: • ANSI • China • ITU • NTT • TTC
Network Indicator	Determines the type of call. Valid values are: • National—National-bound call. The MWTM routes national calls through the national network. • NationalSpare—National-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates networks. • International—International-bound call. The MWTM forwards international-bound calls to an STP pair that acts as an international gateway. • InternationalSpare—International-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates networks
Network Name	Name of the network associated with the signaling point.

Polling Information

The Polling Information section for nodes contains:

Field	Description
Process Traps	Indicates whether traps are processed. To change this setting, check or uncheck the check box in the Process Traps column of the Nodes table.
Trap Polling	Indicates whether trap polling is enabled or not. For IPRAN or mSEF nodes, if you want to: • Enable trap polling, set ipran-mib snmp-access to outOfBand on the node. • Disable trap polling, set ipran-mib snmp-access to inBand on the node. Note For information about in-band and out-of-band management, see RAN-O Specific FAQs, page C-17.
Report Polling	Indicates whether report polling is enabled or not. For IPRAN or mSEF nodes, if you want to: • Enable trap polling, set ipran-mib snmp-access to outOfBand on the node. • Disable trap polling, set ipran-mib snmp-access to inBand on the node. Note For information about in-band and out-of-band management, see RAN-O Specific FAQs, page C-17.
First Discovered	Date and time that the MWTM first discovered the node.
Last Poll IP Address	Last IP address that was polled for this node. For an unmanaged node, this field is blank.
Last Full Poll Time	Date and time of the last full poll of the node for node-related MIBs (as opposed to a demand poll for just one associated object's data). For a node that is not an ITP, IPRAN, or mSEF node, this field is blank.
Last MWTM Poll Response (secs)	Time, in seconds, taken by this node to respond to the last MWTM poll request. For a node that is not an ITP, IPRAN, or mSEF node, this field is blank.
Avg. MWTM Poll Response (secs)	Average time, in seconds, taken by this node to respond to MWTM poll requests. For a node that is not an ITP, IPRAN, or mSEF node, this field is blank.

Protection Information

The Protection Information section for ONS nodes and cards contains:

Column	Description
Card Type	The type of card. This column appears only when you select the ONS node in the navigation tree.
Protected Slot	Slot number of the protected card, which is configured for protection. ¹
Protecting Slot	Slot number of the card that is protecting one or more cards.
Configured State	The configured state of the chosen card: Working or Protecting. The card is working normally or protecting another card.
Current State	The current state of the chosen card: Active or Standby.

1. See the *Cisco ONS 15454 Product Overview* for information about protection schemes for ONS cards:
<http://www.cisco.com/univercd/cc/td/doc/product/ong/15400/45431po.htm>

QoS Information

The QoS Information section for ITP signaling points contains:

Column	Description
QoS	Quality of service (QoS) class of the signaling point. Valid QoS classes range from 1 through 7 . ALL indicates that the signaling point accepts all QoS classes.
ToS	Type of service (ToS) of the signaling point.
DSCP	IP differentiated-services-code-point (DSCP) of the signaling point.

RAN Information



Note

This subsection appears only for configured RAN interfaces (GSM Abis and UMTS Iub interfaces).

The RAN Information section contains:

Field	Description
Protocol	Protocol of the interface (GSM-Abis or UMTS-Iub).
Local IP Address	IP address of the local node.
Local Port	Local port that the interface uses.
Remote IP Address	IP address of the remote (peer) node.
Remote Port	Remote port that the interface uses.

Remote IP Address Information

The Remote IP Address Information section for ITP application server process associations, SCTP links, and signaling gateway mated pairs contains:

Field	Description
IP Address	Remote IP address associated with the object.
Type	Indicates whether this designated primary IP address is for the object (Primary), or is the IP address currently being used by the object (Effective), or both (Primary and Effective). Usually, the same IP address is Primary and Effective. However, if the primary IP address is down for some reason, the object uses a different IP address and is labeled Effective.
Status	Current status of the IP address. Possible values are:  Active —The IP address is currently fully functional.  Inactive —The IP address is not currently functional.
Cfg	(12.2(4)MB10 and later) Indicates whether this remote IP address was configured for the object. Possible values are: • Yes—This is the configured remote IP address, and the object is currently using it. • (blank)—This is not the configured remote IP address. • N/A—The MWTM cannot determine whether this is the configured remote IP address. For Cisco IOS software releases prior to 12.2(4)MB10, this field always displays N/A.
Actual	Indicates whether the object is currently using this remote IP address. Possible values are: • Yes—The object is using the IP address. • (blank)—The object is not using the IP address.

Uptime Information

The Uptime Information section for nodes contains:

Field	Description
Uptime	Time the node is up, in days, hours, minutes, and seconds.
Reboot Reason	Reason for the last reboot of the node.

Status Information

The Status Information section applies to these objects:

- [Nodes, page 8-29](#)
- [Interfaces and Cards, page 8-30](#) (includes RAN backhauls and shorthauls)

- [ITP Application Servers, page 8-34](#)
- [ITP Application Server Processes, page 8-35](#)
- [ITP Application Server Process Associations, page 8-36](#)
- [ITP Links, page 8-38](#)
- [ITP Linksets, page 8-39](#)
- [ITP Signaling Gateway Mated Pairs, page 8-40](#)
- [ITP Signaling Points, page 8-42](#)

Nodes

The Status Information section for nodes contains:

Field	Description
Is Ignored	Indicates whether the node is Ignored (that is, whether to include the node when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”
MTP3 Offload (ITP only)	Indicates whether MTP3 offload is configured for the node. Possible values are: • Main—The MTP3 management function operates only on the main processor. • Offload—The MTP3 management function operates on the main processor and on other available processors. • N/A—MTP3 offload cannot be determined.
NSO Status (ITP only)	Current NSO status of the node, with a color-coded background. Possible values are:  Local—NSO is configured and the secondary peer is in the appropriate status for failover support.  Local—NSO is configured, but the secondary peer is <i>not</i> in the appropriate status for failover support.  None—The node and MIB support NSO, but NSO is not configured on the ITP.  N/A—The node and MIB do not support NSO, or the MWTM cannot determine the NSO status.

Field	Description
Status	Current status of the node. Possible values are:  Active  Discovering  Polling  Unknown  Unmanaged  Waiting  Warning For detailed definitions of each status, see Status Definitions for Signaling Gateway Mated Pairs, page E-7.
Last Status Change	Date and time that the status of the node last changed.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If: • You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

Interfaces and Cards

The Status Information section for interfaces (including RAN backhaul and shorthaul interfaces) and cards contains:

Field	Description
Is Ignored	Indicates whether the interface or card is Ignored (that is, whether the interface or card should be included when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”

Field	Description
Admin Status	Displays the administrative status of the interface. Status can be:  Unknown—Unknown administrative status.  Up—Administratively up.  Shutdown—Administratively down.  Testing—Administrator is testing the interface.
Operational Status	Displays the operational status of the interface. Status can be:  Unknown—Unknown operational status.  Up—Interface is up.  Down—Interface is down.  Testing—Interface is in test mode.  Dormant—Interface is dormant.  Not Present—An interface component is missing.  Lower Layer Down—An interface is down because of a lower-layer interface.
Connect State (for GSM Abis)	Displays the connection state of a GSM interface. States can be:  Connected—The node is monitoring local and remote alarm status.  Disconnected—The system ignores the local alarm status. The local transmitter on the shorthaul is disabled. Capability messages are transmitted to the remote describing the provisioning. The system stays disconnected until the remote capabilities are known and the peer state is transitioning to connected.  Send Connect—One or more attempts have been made to connect to remote peer.  Receive Connect—The local-peer has received a connect request from the remote-peer.  Connect Rejected—Connection was rejected.  ACK Connect—The initial connect request was sent and acknowledged by remote-peer. The local-peer is now waiting for a connect request from the remote-peer.  Check Connect—The local peer has reason to believe its remote peer has failed. Additional tests are being processed to verify peer's state.

Field	Description
Connect State (for UMTS Iub)	Displays the connection state of a UMTS interface. States can be:  Initialized—The connection is starting initialization.  Starting—The shorthaul interface is administratively active, but the backhaul interface is down.  Closed—The backhaul interface is active, but the shorthaul is administratively closed.  Stopped—Unable to connect to peer in specified time interval. Additional attempts will be tried based on peer request or restart timers.  Closing—Connection closed by administration request.  Stopping—Connection shut down by peer's Term-Request. Will transition to stopped state.  Connect Sent—Connection request sent to peer.  ACK Received—Connection request sent and acknowledgement is received from peer. Now waiting for peer's connection request.  ACK Sent—Connection request received and acknowledgement is sent to peer. Connection request sent and waiting for peer's acknowledgement.  Open—Connection open and available for traffic.
Local Receive Alarm State Local Transmit Alarm State Remote Receive Alarm State Remote Transmit Alarm State (for UMTS Iub)	Displays alarm states for UMTS Iub interface. States can be:  Remote Alarm—Indicates a problem at the remote end. The remote interface in the E1/T1 data stream generates and sends the alarm, and no other action is required.  No Alarm—No alarm is present.  Local Alarm—Indicates local interface problem. The interface has not received synchronization from the GSM node. The node stops transmitting backhaul samples.  Received Alarm—Indicates receive problem in the local node. The remote node stops transmitting backhaul data and indicates a blue alarm.  Alarm State Unavailable—Indicates the alarm state is not available. This state only applies to the remote and occurs when the peer connection is inactive.

Field	Description
Local State Remote State (for GSM Abis)	Displays alarm states for GSM Abis interface. States can be:  Remote Alarm—Indicates a problem at the remote end. The remote interface in the E1/T1 data stream is generates and sends the alarm, and no other action is required.  No Alarm—No alarm is present.  Local Alarm—Indicates local interface problem. The interface has not received synchronization from the GSM node. The node stops transmitting backhaul samples.  Received Alarm—Indicates receive problem in the local node. The remote node stops transmitting backhaul data and indicates a blue alarm.  Alarm State Unavailable—Indicates the alarm state is not available. This state only applies to the remote and occurs when the peer connection is inactive.
Redundancy State	Displays information about the GSM Abis or UMTS Iub interface redundancy state. States can be:  Active—Active owner of interface.  Standby—Active owner of interface.
Status	Current status of the interface or card. Possible values are:  Active  Discovering  Down  Polling  Unknown  Unmanaged  Waiting  Warning For detailed definitions of each status, see Status Definitions for Signaling Gateway Mated Pairs, page E-7.

Field	Description
Last Status Change	Date and time of last change to status.
Status Reason	Reason for the current status of the interface or card. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If: - You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOSgm/apache/share/htdocs/eventHelp</i> directory. - You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

ITP Application Servers

The Status Information section for ITP application servers contains:

Field	Description
Is Ignored	Indicates whether the application server is Ignored (that is, whether the application server should be included when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”
Mate Status	Current status of the application server on the signaling gateway mate. Possible values are:  Active  Down  Inactive  Pending  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Application Servers, page E-4.

Field	Description
Last Status Change	Date and time that the status of the application server last changed.
Status	Current status of the application server. Possible values are:  Active  Down  Inactive  Pending  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Application Servers, page E-4.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. To: - You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. - You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

ITP Application Server Processes

The Status Information section for ITP application server processes contains:

Field	Description
Is Ignored	Indicates whether the application server process is Ignored (that is, whether to include the application server process when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”

Field	Description
Last Status Change	Date and time that the status of the application server process last changed.
Status	Current status of the application server process. Possible values are:  Unknown  Unmanaged For detailed definitions of each status, see Status Definitions for Application Server Processes, page E-4.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. To: - You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOs/gm/apache/share/htdocs/eventHelp</i> directory. - You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

ITP Application Server Process Associations

The Status Information section for ITP application server process associations contains:

Field	Description
Is Ignored	Indicates whether the application server process association is Ignored (that is, whether the application server process association should be included when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”
Congestion Level	Indicates the level of congestion on the application server process association. An application server process association is congested if it has too many packets waiting to be sent. This condition could be caused by the failure of an element in your network. Possible values for the Congestion Level field are None, indicating no congestion, and 1 to 7, indicating levels of congestion from very light (1) to very heavy (7).

Field	Description
Instance Status	Current status of the protocol associated with the application server process, with a color-coded background. Possible values are:  Active—The protocol is available.  Shutdown—An administrator has forced the protocol to an unavailable state.  Unknown—The MWTM cannot determine the current status of the protocol.
Status	Current status of the application server process association. Possible values are:  Active  Blocked  Down  Inactive  Pending  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Application Server Process Associations, page E-4.
Last Status Change	Date and time that the status of the application server process association last changed.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. To: - You installed the MWTM in the default directory, <i>/opt</i>, then the file is located at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. - You installed the MWTM in a different directory, then the help directory and file are located in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

ITP Links

The Status Information section for ITP links contains:

Field	Description
Is Ignored	Indicates whether the link is Ignored (that is, whether the link should be included when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”
Last Status Change	Date and time that the status of the link last changed.
Status	Current status of the link. Possible values are:  Active  Blocked  Failed  InhibitLoc  InhibitRem  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Links, page E-6.
Status Reason	Reason for the current status of the link. For a full list of possible reasons, see the <i>stateReasons.html</i> file. To: • You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

Field	Description
Congestion Level	Indicates the level of congestion on the link. A link is congested if it has too many packets waiting to be sent. This condition could be caused by the failure of an element in your network. Possible values for the Congestion Level field are None, indicating no congestion, and 1 to 7 , indicating levels of congestion from very light (1) to very heavy (7).
Receive Utilization	Indicates whether, on average, the link is under its configured receive utilization threshold (UnderThreshold) or over the threshold (OverThreshold).
Send Utilization	Indicates whether, on average, the link is under its configured send utilization threshold (UnderThreshold) or over the threshold (OverThreshold).

ITP Linksets

The Status Information section for ITP linksets contains:

Field	Description
Is Ignored	Indicates whether the linkset is ignored (that is, whether the linkset should be included when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”
Last Status Change	Date and time that the status of the linkset last changed.

Field	Description
Status	Current status of the linkset. Possible values are:  Active  Shutdown  Unavailable  Unknown  Warning For detailed definitions of each status, see Status Definitions for Linksets, page E-7.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. To: • You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons appear(s) in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

ITP Signaling Gateway Mated Pairs

The Status Information section for ITP signaling gateway mated pairs contains:

Field	Description
Is Ignored	Indicates whether the signaling gateway-mated pair is Ignored (that is, whether the signaling gateway-mated pair should be included when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”
Congestion Level	Indicates the level of congestion on the signaling gateway-mated pair. A signaling gateway-mated pair is congested if it has too many packets waiting to be sent. This condition could be caused by the failure of an element in your network. Possible values for the Congestion Level field are None, indicating no congestion, and 1 to 7, indicating levels of congestion from very light (1) to very heavy (7).

Field	Description
Instance Status	Current status of the protocol associated with the signaling gateway-mated pair, with a color-coded background. Possible values are:  Active—The protocol is available.  Shutdown—An administrator has forced the protocol to an unavailable state.  Unknown—The MWTM cannot determine the current status of the protocol.
Status	Current status of the signaling gateway-mated pair. Possible values are:  Active  Blocked  Down  Inactive  Pending  Shutdown  Unknown  Warning For detailed definitions of each status, see Status Definitions for Application Server Process Associations, page E-4.
Last Status Change	Date and time that the status of the signaling gateway-mated pair last changed.
Status Reason	Reason for the current status of the signaling gateway-mated pair. For a full list of possible reasons, see the <i>stateReasons.html</i> file. To: - You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. - You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

ITP Signaling Points

The Status Information section for ITP signaling points contains:

Column	Description
Is Ignored	Indicates whether the signaling point is Ignored (that is, whether the signaling point should be included when aggregating and displaying MWTM status information).
Alarm Severity	Indicates the alarm severity of the object. See Chapter 9, “Managing Alarms and Events.”
Last Status Change	Date and time that the status of the signaling point last changed.
Status	Current status of the signaling point. Possible values are:  Active  Unknown  Unmanaged  Warning For detailed definitions of each status, see Status Definitions for Signaling Points, page E-7.
Status Reason	Reason for the current status of the signaling point. For a full list of possible reasons, see the <i>stateReasons.html</i> file. To: • You installed the MWTM in the default directory, <i>/opt</i>, then the file is in the <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. • You installed the MWTM in a different directory, then the help directory and file are in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full text in a tooltip. The status reasons are listed in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears.
Status Reason (continued)	If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see the Command Reference, page B-1.

Threshold Information (RAN-O Only)

The Threshold Information section for RAN-O nodes contains:

Field	Description
Acceptable	The percentage threshold setting below which the backhaul utilization is considered acceptable. The default Acceptable threshold is 60 percent. ¹
Warning	The percentage threshold setting beyond which the backhaul utilization issues a warning. Subsequent warnings are issued only if the utilization falls below the Acceptable threshold. The default Warning threshold is 70 percent. ¹
Overloaded	The percentage threshold setting beyond which the backhaul utilization is considered overloaded. Subsequent overload messages are issued only if the utilization falls below the Acceptable threshold. The default Overloaded threshold is 80 percent. ¹

1. To change the default setting, see [Editing Properties for a RAN-O Backhaul](#), page 6-36.

Viewing Troubleshooting



Note

If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.



Tip

For more information about troubleshooting, see the *OSS Integration Guide for the Cisco Mobile Wireless Transport Manager 6.1*.

You can run commands and view output in the Troubleshooting section available from the MWTM client or MWTM Web interface.

To view the Troubleshooting section, in a view in the navigation tree, select an object, then click on the Troubleshooting tab in the right pane.



Note

To see which object types pertain to this tab, see [Appendix A, “Client Object Map Reference.”](#)



Tip

To save the output of all executed commands to a log file, see [mwtm tshootlog](#), page B-77.

Before you can run commands and view output, you must properly configure credentials. You can configure credentials by using the CLI command (see [mwtm addcreds](#), page B-6) or through the MWTM client (see [Configuring Login Credentials](#), page 3-20). If credentials are not configured, the output pane displays this message:

No credentials are available for this node

Troubleshooting Menu and Toolbar

The Troubleshooting section displays these menus and toolbar buttons for the chosen object:

Menu or Toolbar Button	Description
Category	A grouping of related commands. The MWTM provides default categories that you cannot modify. Additional categories are user-defined. You can execute all commands in a category at once by using the Execute Category button. Note To define additional categories and create new commands in categories, see Creating New Troubleshooting Categories and Commands, page 3-23
Command	A command or task within the chosen category. The MWTM provides commands for default categories that you cannot modify. You can execute a chosen command by using the Execute Command button.
Suffix	Filters the output of troubleshooting commands. For example: • include—Includes the lines matching the specified regular expression • exclude—Excludes the lines matching the specified regular expression • begin—Starts the printout at the line matching a regular expression • section—Outputs only the matching sections of the printout Note The suffixes allowed here are those supported by the IOS version.
 Execute Command	Executes the chosen command only. Note If you are using Microsoft Internet Explorer, the scroll bar may change position.
 Execute Category	Executes all commands in the chosen category. Note If you are using Microsoft Internet Explorer, the scroll bar may change position.
 Cancel Execution	Stops any execution process.
 Save Output	Saves output on screen to a file.
 Copy Output	Copies output on screen to the clipboard.
 Print Output	Prints output on screen.
 Clear Output	Clears all output from the screen.
Output Pane	Pane where command output appears.

Commands That Require Additional User Input

After you click the Execute Command or Execute Category button, some commands prompt you for additional input. Commands that prompt you for additional input have an ellipsis (...) at the end of the command. You must enter valid data, which appears in green as you type. Invalid data appears in red. The MWTM will not execute a command with invalid data. Once you have entered the additional input, you must click one of these buttons:

Button	Description
OK	Executes the chosen command or category of commands. Note If you do not provide input but leave the fields blank, and then click OK, the MWTM skips the command or commands and this message appears: Skipping command. The MWTM lists the commands that you skipped, but executes other commands for which you provided input.
Clear	Removes entered data from all input fields.
Cancel	Removes the input fields from the right pane.

Related Topics

- [Configuring Login Credentials, page 3-20](#)
- [Troubleshooting IOS Commands on the Web, page D-4](#)
- [mwtm addcreds, page B-6](#)
- [mwtm tshootlog, page B-77](#)

Viewing Alarms and Recent Events

To view alarms for an object, in the navigation tree, select the object (for example, a node), then click the Alarms tab in the content area.

To view recent events for an object, in the navigation tree, select the object (for example, an interface), then click the Recent Events tab in the content area.

The table in the content pane displays information about the alarms or recent events associated with the chosen object. The content pane also provides tools to perform tasks, such as setting filters and acknowledging alarms or events.



Note

For managed objects that have peers (RAN backhauls and shorthauls, ITP links and linksets, and signaling-gateway mated pairs), the MWTM displays subtabs to distinguish alarms and recent events for each peer object.

- For descriptions of the table columns, see [Right-click Menus, page 9-16](#).
- For descriptions of alarms and events tools, see [Toolbar Buttons, page 9-14](#).
- To understand the difference between alarms and events, see [Basic Concepts and Terms, page 9-1](#).

Using Provisioning

This section describes how to provision objects using the MWTM web interface and provides examples. For further information, please see the *OSS Integration Guide for the Cisco Mobile Wireless Transport Manager 6.1*.

http://cisco.com/en/US/docs/net_mgmt/mobile_wireless_transport_manager/6.1/developer/guide/mwtmoss.html

Using provisioning through the MWTM Web interface, you can add, modify, and/or delete ITP, PWE3, CSG2, or GGSN objects, as follows:

ITP	Objects	Add	Modify	Delete
	Linksets	Yes	Yes	Yes
	SCTP Links	Yes	Yes	Yes
	MTP2 Links	Yes	Yes	Yes
	HSMTTP2 Links	Yes	Yes	Yes
	HSL Links	Yes	Yes	Yes
	Application servers, including m3ua and sua	Yes	Yes	Yes
	Application server processes, including m3ua and sua	Yes	Yes	Yes
	Local peer objects	Yes	Yes	Yes
	m3ua objects	Yes	Yes	Yes
	sua objects	Yes	Yes	Yes
	Channelized serial interfaces (under T1/E1 controllers)	Yes	Yes	Yes
	Physical serial interfaces	No	Yes	No
	Physical T1/E1 controllers	No	Yes	No
	Physical ATM interfaces	No	Yes	No
	Physical Ethernet, FastEthernet, or GigabitEthernet interfaces	No	Yes	No

IPRAN (PWE3)	Objects	Add	Modify	Delete
	ATM Connect	Yes	Yes	Yes
	CEM Class	Yes	Yes	Yes
	CEM Group	Yes	Yes	Yes
	Interface ATM, ATM IMA, ATM Sub Interface ¹	Yes	Yes	Yes
	Interface BITS	No	Yes	No
	Interface CEM ¹	No	Yes	No
	Interface E1, T1 ¹	No	Yes	No
	Interface FastEthernet, GigabitEthernet ¹	No	Yes	No
	Interface Loopback ¹	Yes	Yes	Yes
	Interface Serial ¹	Yes	Yes	Yes
	Interface SONET ¹	No	Yes	No
	Interface Tunnel ¹	Yes	Yes	Yes
	Interface Virtual CEM ¹	No	Yes	No
	Module RTM ¹	No	Yes	No
	Node ¹	No	Yes	No
	PVC ¹	Yes	Yes	Yes
	PVP ¹	Yes	Yes	Yes
	Pseudowire Class	Yes	Yes	Yes
	Recovered Clock ¹	Yes	Yes	Yes
	Sonet AU4 Tug ¹	No	Yes	No
	Sonet AU4 ¹	No	Yes	No
	Sonet STS ¹	No	Yes	No
	Sonet Tug ¹	No	Yes	No
	Sonet VTG ¹	No	Yes	No
	Sonet CEM Group	Yes	Yes	Yes
	TDM Connect	Yes	Yes	Yes
	TDM Group	Yes	Yes	Yes
	Virtual CEM Group	Yes	Yes	Yes
CSG2	Objects	Add	Modify	Delete
	CSG2	Yes	Yes	Yes
	CSG Map	Yes	Yes	Yes
	CSG Policy	Yes	Yes	Yes
	CSG Content	Yes	Yes	Yes
	CSG Service	Yes	Yes	Yes
	CSG Billing Plan	Yes	Yes	Yes

GGSN R8	Objects	Add	Modify	Delete
	APN	Yes	Yes	Yes
	GPRS Charging Profile	Yes	Yes	Yes
	GPRS Charging Profile Defaults	Yes	Yes	Yes
	GPRS Global Commands	Yes	Yes	Yes
	Service Mode	Yes	Yes	Yes
	Test by IMSI	Yes	Yes	Yes
	Maximum PDP Contexts	Yes	Yes	Yes
	QoS Default Response Requested	Yes	Yes	Yes
	VRF ¹	Yes	Yes	Yes
	Interface, Loopback ¹	Yes	Yes	Yes
	Interface, Tunnel ¹	Yes	Yes	Yes
	Interface, GigabitEthernet ¹	No	Yes	No
Supervisor of GGSN R8	Objects	Add	Modify	Delete
	L2VLAN ²	Yes	Yes	Yes
	VRF ¹	Yes	Yes	Yes
	Interface, Loopback ¹	Yes	Yes	Yes
	Interface, VLAN ^{1, 2}	Yes	Yes	Yes
	Interface, Tunnel ¹	Yes	Yes	Yes
	Interface, GigabitEthernet ¹	No	Yes	No

1. Not all options and/or subcommands are supported.

2. See bug about VTP Mode Transparent



Note

If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

This section contains:

- [Prerequisites for Using Provisioning, page 8-49](#)
- [Using the Provisioning Wizard, page 8-50](#)

Prerequisites for Using Provisioning

Before you can provision an object:

- You must set up:
 - Basic IP connectivity
 - SNMP community strings
 - Credentials
 - Telnet or SSH access allowed
 - (*ITP only*) Basic signaling points configured
 - (*GGSN only*) The GPRS service must be enabled in IOS
- MWTM must be able to successfully:
 - Discover the object
 - Retrieve running configuration from the object

Setting Up the MWTM to Retrieve Running Configuration from the Object

Before you can use the MWTM to provision objects, you must set up the MWTM to retrieve the running configuration from the object.

The MWTM inventory has two types of attributes:

- **Monitor attributes**—Attributes obtained from SNMP polling and/or status monitoring
- **Configuration attributes**—Attributes obtained from IOS running configuration.

Setting up the MWTM to retrieve running configuration is a two-step process. You must:

1. Supply credentials for the target node(s). For details, see [Configuring Login Credentials, page 3-20](#).
2. Ensure that the MWTM is getting the IOS running configuration successfully from the object. There are two approaches you can use:
 - **Automatic configuration synchronization**—This is the default option. You can verify that the option in the *System.properties* file—look for the AUTO_SYNC_CONFIG field, which should be set to true. If you enable this option, the MWTM automatically retrieves the running configuration from the object after the MWTM processes a provisioning operation (from the GUI or NBAPI). During every status poll, the MWTM checks whether the running configuration has changed on the object. If the configuration has changed, the MWTM retrieves it.
 - **Manual configuration synchronization**—In certain situations, you may choose to turn off automatic configuration synchronization and manage configuration synchronization manually. You can request manual configuration synchronization using the NBAPI or the CLI. For details, see the *OSS Integration Guide for the Cisco Mobile Wireless Transport Manager 6.1*.

Using the Provisioning Wizard



Note

Throughout the wizard, you can click **Next** to continue, **Previous** to go back, **Cancel** to exit the wizard without saving changes, **Refresh** to reload the current window, or **Submit** to complete the provisioning.

To start provisioning by using the MWTM provisioning wizard:

- Step 1** From the MWTM client, right-click a node in the navigation tree and choose **Provision** or
From the MWTM web interface, click a node in the navigation tree and click the **Provision** tab in the content pane.
- Step 2** Select a **Type** (and **SubType**, if applicable).
- Step 3** Click **New** to create a new item of the chosen Type or select an item in the Provisioned Items list, then click **Edit** or **Delete**.

The provisioning wizard appears as shown in [Figure 8-3](#).

Figure 8-3 Provisioning Wizard

There are three possible wizard stages: Basic, Features, and Summary.



Note

If you do not initiate activity on an active wizard screen, your session will time out after 60 seconds, and the MWTM returns to the Provision Choices window.

- Step 4** Enter the relevant information at the Basic stage and click **Next** to continue.
- Step 5** (Optional) Make your selections at the Features stage. Notice that as you enable features, they appear in the Wizard Steps pane under Features. Click **Next** to continue.
- Step 6** (Optional) If you have added features, you can choose to configure aspects of each feature. Click **Next** to continue, or click the wizard stage in the left pane to jump between stages.

- Step 7** The Summary stage appears, showing which IOS commands the MWTM will send to the object. You can optionally check the box **Write to IOS startup-config**, which saves your configuration changes permanently to the startup configuration on the object. This process can take time.
- Step 8** Click **Submit** to send the provisioning to the object.
-

The provisioning wizard provides colored status balls in the Wizard Steps pane, which indicate:

- **White**—The stage you are in currently
- **Red**—A problem in the stage
- **Yellow**—Stage is not yet configured
- **Green**—Stage is configured successfully

Editing SNMP IP Addresses for a Node

You use the MWTM to determine which IP addresses to use for SNMP polling.

To edit a node's SNMP IP addresses, right-click a node in a window, choose **Edit > SNMP IP Addresses** in the right-click menu. The MWTM displays the Edit SNMP IP Addresses dialog box.

The Edit SNMP IP Addresses dialog box contains:

Field or Button	Description
Available IP Addresses	List of all IP addresses associated with this node that users could not or do not want the MWTM to use for SNMP polling. The MWTM does not send SNMP queries to IP addresses in this list. This option appears only for ITP, IPRAN, or mSEF nodes.
IP Addresses for SNMP	List of all IP addresses associated with this node that the MWTM can use for SNMP polling: - By default, the MWTM places all discovered IP addresses in this list, in the order in which they are discovered. The MWTM uses the IP address at the top of the list as the primary SNMP address for the node. During SNMP polling of the node (status polling and demand polling), the MWTM first tries the primary SNMP address. If the primary is unavailable, the MWTM tries the other IP addresses, one-by-one, in descending order. - To assign a new primary SNMP address, or to change the order of the secondary IP addresses, click the Raise Priority and Lower Priority buttons to move the IP addresses up and down in the list. - You can also select IP addresses that you do not want the MWTM to use for SNMP polling. This feature is useful, for example, to separate management traffic from SMS traffic. To remove an IP address from the list, click Remove. The MWTM removes the IP address from the IP Addresses for SNMP list, places it in the Available IP Addresses list, and no longer uses it for SNMP polling. To enable an IP address for SNMP polling again, select the address in the Available IP Addresses list and click Add. The IP address moves back into the IP Addresses for SNMP list and is again available for SNMP polling. If you remove all IP addresses from the IP Addresses for SNMP list, you remove the node from the network, and the MWTM automatically labels the node Unmanaged in all MWTM windows. When you click Save, all MWTM windows are updated automatically to reflect the changes. This option appears only for ITP, IPRAN, or mSEF nodes.
Add	Enables one or more chosen IP addresses for SNMP polling. All chosen IP addresses in the Available IP Addresses list are moved to the IP Addresses for SNMP list where the MWTM uses them again for SNMP polling.
Remove	Disables one or more chosen IP addresses for SNMP polling. All chosen IP addresses in the IP Addresses for SNMP list are moved to the Available IP Addresses list, and are no longer used by the MWTM for SNMP polling.
Raise Priority	Moves the chosen IP addresses up in the IP Addresses for SNMP list. If you move an IP address to the top of the list, the MWTM uses that IP address as the new primary SNMP address for the node.
Lower Priority	Moves the chosen IP addresses down in the IP Addresses for SNMP list. If you remove an IP address from the top of the list, the MWTM no longer uses that IP address as the primary SNMP address for the node.

Field or Button	Description
Save	Saves changes that you made to the node information and exits the dialog box. When you are satisfied with your changes, click Save . The MWTM saves your changes and updates all MWTM windows to reflect your changes.
Cancel	Exits the dialog box without saving any changes. At any time, you can click Cancel to exit the dialog box without saving any changes.
Help	Displays online help for the dialog box.

Polling a Node

The MWTM automatically polls nodes at specified intervals. However, you can also request an immediate poll for a node. This section describes:

- [Polling from the Discovery Dialog, page 8-53](#)
- [Performing a Normal Poll, page 8-54](#)
- [Performing a Clean Poll, page 8-55](#)

Polling from the Discovery Dialog

To poll a node from the Discovery dialog box:

Step 1 Choose **Network > Network Discovery** from the MWTM main menu.

The MWTM displays the Discovery dialog box.

Step 2 Select the Discovery tab.

The MWTM displays the Discovery pane. The Discovered Nodes section of the Discovery pane lists all discovered nodes (all nodes, including new and excluded nodes, not just the nodes in the current view).

Step 3 Select one or more nodes.



Note You cannot poll a node with a Primary SNMP Address of N/A. If you select a node with a Primary SNMP Address of N/A, then the Poll Node button is dimmed and cannot be chosen. If you select more than one node, and even one of them has a Primary SNMP Address of N/A, then the Poll Node button is dimmed and cannot be clicked.

Step 4 Click **Poll Node**.

The MWTM begins a poll of the chosen nodes. During polling, the Poll Node button is dimmed, the *Selected nodes are being polled* message appears at the bottom of the Discovery dialog box, and individual nodes might display the polling status.



Note If the node has only one IP address for the MWTM to poll, and the poll fails or times out, the MWTM issues an error message. If the node has more than one IP address for the MWTM to poll, and the polls of one or more IP addresses fail or time out, the MWTM issues warning messages. If all polls fail or time out, the MWTM issues an error message.

When the `Selected nodes are being polled` message disappears and no nodes are in polling status, polling is complete. The MWTM database immediately reflects any new or changed data for the chosen nodes.

Performing a Normal Poll

A normal poll retains all objects associated with polled nodes, even objects that have been deleted and are therefore in Unknown status.

To poll one or more nodes, retaining all associated components in the MWTM database, use one of these procedures:

From a View in the Main Window

- Step 1** Select a view in the navigation tree.
 - Step 2** Select one or more nodes in the navigation tree.
 - Step 3** Choose **Network > Poll Nodes > Normal Poll**.
- The MWTM polls all chosen objects.
-

From Summary Lists

- Step 1** Click **Nodes** under Summary Lists in the navigation tree.
 - Step 2** Select a node or adjacent node in the node table in the right pane.
 - Step 3** Choose **Network > Poll Nodes > Normal Poll**.
- The MWTM polls that node.
-

From Rick-click Menu in a View

- Step 1** Select a view in the navigation tree.
 - Step 2** Right-click a node in the navigation tree.
 - Step 3** Choose **Poll Node > Normal Poll** from the right-click menu.
- The MWTM polls the node.
-

Performing a Clean Poll

A clean poll removes all network objects from the node at the completion of the poll.

To poll one or more nodes, removing and then rediscovering all associated components, use one of these procedures:

From a View in the Main Window

-
- Step 1** Select a view in the navigation tree.
 - Step 2** Select one or more nodes in the navigation tree.
 - Step 3** Choose **Network > Poll Nodes > Clean Poll**.
The MWTM polls all chosen nodes.
-

From Summary Lists

-
- Step 1** Click **Nodes** under Summary Lists in the navigation tree.
 - Step 2** Select a node or adjacent node in the node table in the right pane.
 - Step 3** Choose **Network > Poll Nodes > Clean Poll**.
The MWTM polls that node.
-

From Rick-click Menu in a View

-
- Step 1** Select a view in the navigation tree.
 - Step 2** Right-click a node in the navigation tree.
 - Step 3** Choose **Poll Node > Clean Poll** from the right-click menu.
The MWTM polls the node.
-

Clean Node for ITP Objects

-
- Step 1** Select a view in the navigation tree.
 - Step 2** Select an application server, application server process, link, or linkset in the navigation tree or in the Summary Lists tables.
 - Step 3** Choose **Network > Poll Nodes > Clean Poll**.
The MWTM polls all ITP nodes and adjacent nodes associated with the object.
-

Allowing and Disallowing Trap Processing for a Node

By default, the MWTM processes traps from all discovered nodes. However, you can prevent the MWTM from processing traps from one or more nodes. For example, if a node is experiencing many link changes and generating too many traps, you can disallow traps from that node until the situation stabilizes.



Note

If you prevent the MWTM from processing traps from a node, all MWTM clients and views connected to that MWTM server are prevented from processing traps from that node.

Also, if you prevent the MWTM from processing traps from a node, make a note of the change, and remember to reset the node when the problem is corrected or the maintenance is complete.

To prevent the MWTM from processing traps from a node, use one of these procedures:

- Uncheck the **Process Traps** check box for the node in the Node table.



Note

By default, the Process Traps column is hidden. To display the Process Traps column, right-click in the table heading and select the **Process Traps** check box.

- Right-click the node in the navigation tree, then choose **Disallow Trap Processing**.

To allow the MWTM to process traps from a node, use one of these procedures:

- Check the **Process Traps** check box for the node in the Node table.
- Right-click the node in the navigation tree, then choose **Allow Trap Processing**.

Viewing Real-Time Data

You can use the MWTM to view real-time data for chosen objects in the navigation tree. The real-time statistics for some objects (CSG2, BWG, HA, and GGSNs on SAMI cards) appear only in the MWTM web interface (see [Chapter 11, “Accessing Data from the Web Interface”](#) to view these statistics).



Note

In the MWTM client, the real-time icon  appears in some tabs in the right pane. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

For more information on viewing real-time data, see:

- [Viewing the Syslog, page 8-57](#)
- [Viewing CPU Performance, page 8-58](#)
- [Viewing Trap Settings, page 8-62](#)
- [Viewing Data for Interfaces, page 8-63](#)
- [Viewing Data for ITP Objects, page 8-66](#)
- [Viewing ITP MTP3 Errors, page 8-93](#)
- [Viewing ITP MSU Rates, page 8-94](#)
- [Viewing ITP Non-Stop Operation, page 8-95](#)

- [Viewing TDM Statistics, page 8-103](#)
- [Viewing RAN-O Performance Data, page 8-107](#)
- [Viewing RAN-O Error Data, page 8-115](#)
- [Viewing PWE3 Statistics, page 8-121](#)

Viewing the Syslog

The Syslog section displays all messages in the system log for the chosen node.



Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

To view the Syslog section, in a view in the navigation tree, select a node, then click the Syslog tab in the content area.

The Syslog section displays these columns for the chosen node:

Column	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Timestamp	Date and time of the syslog message from the node.
Severity	Severity of the syslog message. Possible values are: • Alert—Conditions that require immediate action. • Critical—Critical conditions. • Debug—Debug conditions, log FTP commands, and WWW URLs. • Emergency—System unusable conditions. • Error—Error conditions. • Info—Information conditions. • Notice—Normal but significant conditions. • Warning—Warning conditions.
Facility	Name of the facility that generated the syslog message, such as SYS, SNMP, CS7MTP3, or CS7PING.
Name	Short text identifier for the message type. A facility name in conjunction with a message name uniquely identifies a syslog message type.
Message	Text of the syslog message.

Viewing CPU Performance

The Performance tab provides real-time chart and table statistics about:

- [CPU Processes, page 8-58](#)
- [CPU Utilization, page 8-59](#)
- [Memory Utilization, page 8-60](#)

**Note**

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

To view real-time CPU performance statistics, in a view in the navigation tree, select a node, then click the Performance tab in the content area. The Performance tab appears in the right pane when you select any of these nodes: CSG1, CSG2, GGSN, BWG, CSR, HA, RAN-SVC, ITP.

**Note**

In some cases, users can notice a difference in the number of CPUs reported by the CPU Utilization, CPU Processes, and Memory Utilization selections. The CPU MIBs do not report statistics for cards that are in standby mode (for example, supervisor cards). However, the memory MIB does report memory utilization for standby cards. Because of this difference, the Memory Utilization selection can display a greater number of CPUs than the CPU Utilization and CPU Processes selections.

Also, because the information for memory and CPU statistics comes from different MIBs, the CPU descriptions can vary. Users can correlate the information by comparing the descriptions available among the CPU Utilization, CPU Processes, and Memory Utilization selections. Devices that support the CISCO-MEMORY-POOL-MIB show only the description of the main processor.

CPU Processes

To view real-time CPU processes for the node, click the View drop-down arrow in the MWTM client or MWTM web interface, and select **CPU Processes**.

The MWTM client displays information about CPU processes in a table with slot- and CPU-specific tabs. When you click the tabs for a specific slot and CPU, the MWTM shows CPU process information for the selected CPU. If only a single CPU exists, no tabs for slots or CPUs appear. The MWTM displays information for the CPU in the right pane.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

Each table contains:

Field or Column	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
PID	Process identifier.

Field or Column	Description
Name	Name of the process.
Time Created	Total time since the process was created.
Total Runtime	CPU time the process has used.
Times Invoked	Number of times the process was invoked.
Average Runtime	Average CPU time for each process invocation.
5 Sec %	Average CPU utilization percentage for the node over the last 5 seconds.
1 Min %	Average CPU utilization percentage for the node over the last minute.
5 Min %	Average CPU utilization percentage for the node over the last 5 minutes.
Priority	Process queue priority. Possible values are: • Low • Normal • High • Critical

CPU Utilization

To view real-time CPU utilization for the node, click the View drop-down arrow in the MWTM client, and select **CPU Utilization**.

The MWTM client displays a CPU utilization chart with:

- A Summary tab that shows the combined utilization of all CPUs on the node
- Slot- and CPU-specific tabs that show utilization for a selected CPU



Note

The MWTM web interface displays this data in tabular, instead of chart, format. To view the tabular data in its raw format, in the *Server.properties* file, set the `WEB_DEBUG` parameter to true.

The CPU summary chart displays a vertical band whenever at least one its CPUs is above the normal threshold. Status balls on the CPU-specific tabs indicate the highest threshold status of all data series for the CPU for the last polling interval.

The CPU-specific charts display horizontal bands to show overloaded, warning, and acceptable thresholds; you must configure the CPU rising and falling thresholds on the device to display these bands in the MWTM. The falling threshold corresponds to the boundary between the acceptable and warning bands. The rising threshold corresponds to the boundary between the warning and overloaded bands. For multi-CPU devices, these thresholds apply only to the main CPU.

GUI Elements	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Poll Interval	Label that shows the current poll interval in seconds.
Percentage	Y-axis label that shows percentage of CPU utilization over time.

GUI Elements	Description
Time	X-axis label that displays a real-time scale and the server time zone.
Legend	Identifies the data series currently showing in the chart. 5 sec—Average CPU utilization percentage for the node over the last 5 seconds. 1 min—Average CPU utilization percentage for the node over the last minute. 5 min—Average CPU utilization percentage for the node over the last 5 minutes. - No Data—Color-coded value that indicates no data is available to display. - CPU Threshold Crossed—In the Summary-tab chart, color-coded value that indicates when CPU utilization is above normal. - Overloaded—In a CPU-tab chart, color-coded value that indicates when CPU utilization is in the overloaded zone. - Warning—In a CPU-tab chart, color-coded value that indicates when CPU utilization is in the warning zone. - Acceptable—In a CPU-tab chart, color-coded value that indicates when CPU utilization is in the acceptable zone.

Memory Utilization

To view CPU memory utilization for the node, click the View drop-down menu in the MWTM client or MWTM web interface, and select **Memory Utilization**.

The MWTM client displays memory utilization in a table with:

- A Summary tab that shows the combined memory utilization of all CPUs on the node
- Slot- and CPU-specific tabs that show memory utilization for a selected CPU



Note

Depending on the device, memory utilization statistics may not be available from the management information base (MIB). Devices that support the CISCO-ENHANCED-MEMORY-POOL-MIB have detailed memory information for each CPU. Devices that support the CISCO-MEMORY-POOL-MIB have memory information only for the CPU of the main processor. For these devices, the memory utilization table shows only one entry even though these devices can have multiple CPUs. In these cases, the CPU Description column indicates *CPU of main processor*.

Summary Tab

The Summary tab displays a tabular overview of all CPUs in the chosen node to enable users to easily observe problem areas.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Summary table.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Summary table contains:

Field or Column	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
CPU	Slot number (if known) and CPU number.
CPU Description	Type of CPU.
Processor Memory	Percentage of available processor memory in use.
I/O Memory	Percentage of available I/O memory in use.

CPU-specific Tabs

The CPU-specific tabs display tabular information for the selected slot and CPU. If only a single CPU exists, no slot or CPU tabs appear and the MWTM displays the information for the CPU in the right pane.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

Each CPU-specific table contains:

Field or Column	Description
Poll Interval	Poll interval used to collect data for the table. Note Polling for memory statistics takes longer than for CPU statistics. If excessive timeouts occur for memory polling, you can increase the number of milliseconds for the timeout by changing the <code>MEMORY_POLLER_TIMEOUT_INCREMENT</code> in the <i>Server.properties</i> file.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Memory Type	The type of memory, either processor memory or I/O memory.
Utilization	Percentage of utilization for each type of memory.
Total	Total amount of memory for each memory type.
Used	Amount of memory that is used for each memory type.
Free	Amount of free (unused) memory for each memory type.
Largest Free ¹	The largest available memory unit.
Valid ¹	Whether or not the memory is valid for use.

1. This column is hidden by default. Right-click in the column header and check the check box next to the heading label to display it.

Viewing Trap Settings

The Trap Settings section displays all trap settings for the chosen node, as well as all hosts and port numbers to which the node sends traps.

If you have implemented MWTM User-Based Access, this option is available to users with authentication level 5 (System Administrator).



Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

To view the Trap Settings section, in a view in the navigation tree, select a node, then click on the Trap Settings tab in the content area.

The Trap Settings section displays these columns for the chosen node:

Column	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Release 2 Trap Settings (ITP only)	Indicates whether these ITP release 12.2(4)MB4 trap settings are enabled: • SCTP Remote Address Change • Linkset State Change • Link State Change • Link Congestion State Change • Link Receive Utilization Change • Link Send Utilization Change • Route State Change • GTT MAP State Change
Release 3 Trap Settings (ITP only)	Indicates whether these ITP release 12.2(4)MB5 through 12.2(4)MB9a trap settings are enabled: • ASP State Change • AS State Change • SGMP State Change This column might not be visible if the ITP does not support ITP release 12.2(4)MB5 through 12.2(4)MB9a traps.

Column	Description
Release 4 Trap Settings (ITP only)	Indicates whether these ITP release 12.2(4)MB10 through 12.2(20)SW trap settings are enabled: • Linkset State Change • Link State Change • Link Congestion State Change • Link Receive Utilization Change • Link Send Utilization Change • Route Destination State Change • Route Mgmt. State Change • Route Table Load • GTT MAP State Change • GTT Table Load • ASP Congestion Change • SNMP Congestion Change This column might not be visible if the ITP does not support ITP release 12.2(4)MB10 through 12.2(20)SW traps.
Release 6 Trap Settings (ITP only)	Indicates whether the following ITP release 12.2(25)SW3 trap setting is enabled: • MLR Load Table This column might not be visible if the ITP does not support ITP release 12.2(25)SW3 traps.
RAN Trap Settings (RAN-O only)	Trap settings for the node. These settings include: • GSM State Change • UMTS State Change
Local IP Address	IP address of a local host to which the node sends traps.
Port	Port to which the node sends traps.
Trap Version	Trap version sent to this IP address and port.
Community String	SNMP community name used by the node for read access to the information maintained by the SNMP agent on the node.

Viewing Data for Interfaces



Note

The MWTM client provides charts and tables to display the performance and error information for the chosen interface. The MWTM web interface displays the same information in a tabular format.

For most interfaces, the MWTM displays interface performance and error information in separate tabs in the right pane. However, depending on variables such as node type, card type, interface type, IOS software image, and the running configuration on the node itself, performance and error statistics may not be available for the chosen interface.

**Note**

- Interface performance and error statistics are not available for T1, E1, Synchronous Digital Hierarchy (SDH), or RAN-O shorthaul interfaces.
- Statistics are also unavailable for these ATM interface types: ATM subinterface and ATM layer.

For the chosen interface, you can view:

- [Real-Time Interface Performance, page 8-64](#)
- [Real-Time Interface Errors, page 8-65](#)

Real-Time Interface Performance

To view real-time interface performance, select the interface in the navigation tree, then click the Interface Performance tab.

**Note**

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

You may be prompted to start an in-band poller if polling cannot be done out of band.

The Interface Performance tab contains:

GUI Element ¹	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Poll Interval	Label that shows the current poll interval in seconds.
Last Poll	Label that identifies when the last poll occurred.
Bits or Bytes/Sec (MWTM client) or Current Rate (MWTM web interface)	MWTM client: The MWTM displays separate charts for send (out) and receive (in) traffic on the chosen interface. The Y-axis label that displays the interface traffic rate in bits or bytes per second. The default is bits per second. To change the charts to show bytes per second, uncheck the Show Details in Bits instead of Bytes check box in the Preferences window (General Display Settings, page 5-4). The Y axis automatically scales to the interface speed. MWTM web interface: Displays the interface traffic rate in bits or bytes per second.
% Utilization	For interface speeds greater than zero, the right side of the Y axis displays the percent utilization of the interface, on a scale from 0 to 100%.
Time	X-axis label that displays a real-time scale and the server time zone.

GUI Element ¹	Description
Legend	Identifies the data series currently showing in the chart. • Out—Shows the outgoing (transmit) traffic rate of the chosen interface. • In—Shows the incoming (receive) traffic rate of the chosen interface. • No Data—Data is not available. A vertical bar appears in the chart.
Show/hide right-click menu	Provides options to show or hide one or more parts of a data series. See Right-click Menu, page 8-95 , for descriptions of the options.
(MWTM Web only) Total Count Since Reboot (bits)	Total number of bits since reboot.
(MWTM Web only) Interface Speed (bits/sec)	Interface send and receive speed in bits per second.

1. The MWTM web interface displays the same information in tabular, not chart, format.

Real-Time Interface Errors

To view real-time interface errors, select the interface in the navigation tree, then click the Interface Errors tab.



Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data. You may be prompted to start an in-band poller if polling cannot be done out of band.

The Interface Errors tab contains:

GUI Element	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Reset Counters	Opens the Reset Counters dialog box to configure the method of polling. See Changing Real-Time Poller and Counter Settings, page 5-21 .
Poller Counter Mode	Label that displays the polling mode that you configure in the Reset Counters dialog box.
Poll Interval	Label that shows the current poll interval in seconds.
Last Poll	Label that identifies when the last poll occurred.

GUI Element	Description
Interface Errors	Table that shows this information for the chosen interface: • Data Type: – In Errors—Incoming (receive) errors. – Out Errors—Outgoing (transmit) errors. – In Discards—Incoming, discarded packets. – Out Discards—Outgoing, discarded packets. – Unknown Protocol Packets Received—For packet-oriented interfaces, the number of received packets that were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of received transmission units that were discarded because of an unknown or unsupported protocol. For interfaces that do not support protocol multiplexing, the count will always be 0. • Counts—Error counts since the last reboot. • Rates (per sec)—Error rates since the last reboot.
Output Queue Size	The length of the output packet queue (in packets). When a router receives a packet, it typically forwards it to another interface. The packet enters a queue on the output interface before it is actually sent. The interface typically has a buffer that can hold a fixed number of packets in the queue. When the output queue overflows, the router begins to discard packets.
Interface Errors / Sec	Chart that shows interface errors per second for the chosen interface. The Y axis shows errors per second. The X axis shows a real-time scale and the server time zone. A legend provides color-coded descriptions of the error types for the incoming and outgoing traffic. Note This chart is only available in the MWTM client interface. The MWTM web interface shows the same data in tabular format.

Viewing Data for ITP Objects

You use the MWTM to view detailed statistics for any of these ITP objects:

- Application Servers
- Application Server Process Associations
- Links
- Linksets
- Signaling Gateway Mated Pairs

To display detailed statistics for an object:

- In the MWTM client—In a view in the navigation tree, right-click an object, then choose **View > Real-Time Data and Charts**. The MWTM displays the Statistics Details window for the object.

**Note**

The MWTM server automatically reflects updates for the objects received in this window.

Changes you make in this window might not be reflected throughout the MWTM until the next poll (by default, every 15 seconds). For information about changing the poll interval, see [Poll Settings, page 8-75](#).

- In the web interface—Click on the relevant object (Application Server, Linkset, and so on) in the navigation tree and choose the relevant tab in the content pane.

The Statistics Details window in the MWTM client has a navigation tree, which contains:

Component	Applicable To	Content Links
Poll Settings	All objects	Poll Settings
Right-click menu	Links	Right-Click Menu

The Statistics Details window and the MWTM web interface may contain these tabs in the content pane:

Tab	Applicable To	Content Links
Alarms	All objects	Viewing Alarms and Recent Events
Charts (MWTM client only)	• Application servers • Application server process associations • Links • Linksets	Charts: Application Servers and Application Server Process Associations Charts: Links and Linksets
Details	All objects	Viewing Details
Interface Details	• Application Server Process Associations • Links • Signaling Gateway Mated Pairs	Interface Details
Linkset Access Lists	Linksets	Viewing ITP Linkset Access Lists
Notes	All objects	Viewing Notes
Q.752 Measurements	Links	Q.752 Measurements
Recent Events (MWTM client only)	All objects	Viewing Alarms and Recent Events
SCTP Association Configuration Details	• Application Server Process Associations • Links • Signaling Gateway Mated Pairs	SCTP Association Configuration Details

Tab	Applicable To	Content Links
SCTP Association Statistics Details	- Application Server Process Associations - Links - Signaling Gateway Mated Pairs	SCTP Association Statistics Details
Statistics	- Application Servers - Application Server Process Associations - Links - Linksets	Statistics: Application Servers Statistics: Application Server Process Associations Statistics: Links and Linksets
Status Contributors	Application Servers	Viewing Status Contributors
Status Details	Links	Status Details
Troubleshooting	- Application Servers - Application Server Process Associations - Links - Linksets - Signaling Gateway Mated Pairs	Viewing Troubleshooting

Charts: Application Servers and Application Server Process Associations

You use the MWTM to view real-time MTP3 and ASP packet rate information for the chosen application server or application server process association. To do so, click the Charts tab in the Statistics Details window for an application server or application server process association, then click the relevant tab and the chosen chart appears.

The Statistics Details: Charts section for application servers and application server process associations contains:

Tab	Description	Applicable To
MTP3 Packet Rate	Displays MTP3 packet rate information for a chosen application server.	Application servers
ASP Packet Rate	Displays real-time application server process packet rate information for a chosen application server.	Application servers
Packets From ASP Rate	Displays real-time rate information for packets received by the application server process for the chosen application server or application server process association.	Application servers and application server process associations
Packets To ASP Rate	Displays real-time rate information for packets sent to the application server process by the chosen application server or application server process association.	Application servers and application server process associations

Tab	Description	Applicable To
Packets From MTP3 Rate	Displays real-time rate information for packets received by the chosen application server or application server process association, from the MTP3 layer.	Application servers and application server process associations
Packets To MTP3 Rate	Displays real-time rate information for packets sent to the MTP3 layer from the chosen application server or application server process association.	Application servers and application server process associations

The tabs in the Statistics Details: Charts section for application servers and application server process associations contain:

Field or Button	Description
Time window (mins)	Drop-down list box used to specify the length of time appear in the chosen chart. Valid selections are 1, 2, 5, 10, 20, 40, or 60 minutes. The default selection is 5 minutes.
<Type> Rate Chart	Displays one of these rate charts for the chosen application server or application server process association as a function of time: • MTP3 Packet Rate Chart • ASP Packet Rate Chart • Packets From ASP Rate Chart • Packets To ASP Rate Chart • Packets From MTP3 Rate Chart • Packets To MTP3 Rate Chart
<Type> Rate Chart (continued)	To see the exact time and data coordinates for a data point, left-click the data point. The coordinates appear in the format (<i>hh:mm:ss, dd.dd</i>), where: • <i>hh:mm:ss</i> is the time for that data point in hours, minutes, and seconds. • <i>dd.dd</i> is the MTP3 packet rate for that data point. The Time window (mins) field specifies the total visible time in the chart. New data points are added to the right side of the chart. When the chart reaches the end of the time window (for example, after 5 minutes, if the Time window (mins) field is set to 5), new data points continue to be added to the right side of the chart, while old data points drop off the left side of the chart. If a poll is missed (for example, as a result of an SNMP timeout), the MWTM ignores the missing data point, stops drawing the line, and waits for the next valid data point to begin drawing the line again. To scroll left, right, up, or down in the chart, drag the cursor while holding down Ctrl and the left mouse button. To zoom in on a section of the chart, drag the cursor while pressing Shift and the left mouse button. To reset the chart to the default view and scaling, click Reset.

Field or Button	Description
AS or ASPA	Displays color-coded icons for the application server process associations associated with the application server, or for the application server process association. To add the data for an application server process association to the chart, click the icon in this field. To remove the data from the chart, click the icon again. You use the MWTM to customize the symbols, line styles, and colors assigned to data points in real-time data charts. For more information, see Changing Charts Settings, page 5-11 .
Reset	If you scrolled or zoomed the chart, resets the chart to the default view and scaling.
Grid On	Superimposes a graphic grid on the chart. The grid can make the data easier to read.
Grid Off	Removes the graphic grid from the chart.
Help	Displays online help for the current window.

Charts: Links and Linksets

You use the MWTM to view real-time received, sent, and dropped information for the chosen link or linkset. To do so, click the Charts tab in the Statistics Details window for a link or linkset, then click the relevant tab and the chosen chart appears.

The Statistics Details: Charts section for links and linksets contains:

Tab	Description
ReceivedUtilization	Displays real-time ReceivedUtilization information for the chosen link or linkset.
SendUtilization	Displays real-time SendUtilization information for the chosen link or linkset.
PktsRcvdPerSec	Displays real-time packets-received-per-second information for the chosen link or linkset.
PktsSentPerSec	Displays real-time packets-sent-per-second information for the chosen link or linkset.
BitsRcvdPerSec or BytesRcvdPerSec	Displays real-time bits-received-per-second information for the chosen link or linkset (or bytes-received-per-second information, if you unchecked the Show Details in Bits Instead of Bytes check box in the Preferences window).
BitsSentPerSec or BytesSentPerSec	Displays real-time bits-sent-per-second information for the chosen link or linkset (or bytes-sent-per-second information, if you unchecked the Show Details in Bits Instead of Bytes check box in the Preferences window).
Drops	Displays drops information for the chosen link or linkset.

The tabs in the Statistics Details: Charts section for links and linksets contain:

Field or Button	Description
Linkset	Drop-down list box used to select the linkset from whose perspective data should be visible. By default, data appears from the perspective of the chosen linkset. To display data from the perspective of the adjacent linkset, select it in this list box.
Time window (mins)	Drop-down list box used to specify the length of time visible in the chosen chart. Valid selections are 1, 2, 5, 10, 20, 40, or 60 minutes. The default selection is 5 minutes.
<Type> Chart	Displays one of these charts for the chosen link (and all links on the linkset) or linkset (up to 16 links) as a function of time: • Received Utilization Chart • Send Utilization Chart • Packets Received Chart • Packets Sent Chart • Bits or Bytes Received Chart • Bits or Bytes Sent Chart • Drops Chart To see the exact time and data coordinates for a data point, left-click the data point. The coordinates are visible in the format (<i>hh:mm:ss, dd.dd</i>), where: • <i>hh:mm:ss</i> is the time for that data point in hours, minutes, and seconds. • <i>dd.dd</i> is the receive utilization percentage for that data point. Note (For ReceivedUtilization and SendUtilization only) For serial and HSL links on Cisco 7507 and 7513 series routers, the visible utilization data can vary by up to 5% from the actual utilization—the MWTM might even display utilization data of more than 100%. This variance results from the synchronization of Layer 2 counters between the Versatile Interface Processor (VIP) CPU and the Route Switch Processor (RSP) CPU on 7500 series routers. This variance does not occur for links on Cisco 2600, 7200, or 7300 series routers.

Field or Button	Description
<Type> Chart (continued)	If more than one link appears in the SLC field, you can compare the visible data to that of one or more of the other links by clicking the color-coded icons. To remove the data for the additional links, click the icons again. The Time window (mins) field specifies the total visible time in the chart. New data points are added to the right side of the chart. When the chart reaches the end of the time window (for example, after 5 minutes, if the Time window (mins) field is set to 5), new data points continue to be added to the right side of the chart, while old data points “drop off” the left side of the chart. If a poll is missed (for example, as a result of an SNMP timeout), the MWTM ignores the missing data point, stops drawing the line, and waits for the next valid data point to begin drawing the line again. To scroll left, right, up, or down in the chart, drag the cursor while holding down Ctrl and the left mouse button. To zoom in on a section of the chart, drag the cursor while pressing Shift and the left mouse button. To reset the chart to the default view and scaling, click Reset.
SLC	Displays up to 17 color-coded icons. One for: - Each link (SLC) in the chosen chart, up to 16 total links. - The average of all SLCs. To add the data for a link or for the average to the chart, click the icon in this field. To remove the data from the chart, click the icon again. You use the MWTM to customize the symbols, line styles, and colors assigned to data points in real-time data charts. For more information, see Changing Charts Settings, page 5-11.
Show threshold line for (Linksets only, ReceivedUtilization or SendUtilization)	Draws a horizontal line on the chosen utilization chart, indicating the receive and send threshold for the chosen link. If you do not want to draw a threshold line, select None. This is the default setting.
Scale to threshold (Linksets only, ReceivedUtilization or SendUtilization)	Scales the chosen utilization chart in order to draw the threshold chosen in the Show threshold line for field. To: - Scale the chart, check this check box. - Remove the scaling from the chart, uncheck this check box. This is the default setting. The Scale to threshold check box is not available if the Show threshold line for field is set to None.
Reset	If you scrolled or zoomed the chart, resets the chart to the default view and scaling.
Grid On	Superimposes a graphic grid on the chart. The grid can make the data easier to read.
Grid Off	Removes the graphic grid from the chart.
Help	Displays online help for the current window.

Interface Details

You use the MWTM to view real-time interface details for the chosen application server process association, link, or signaling gateway-mated pair.

The Statistics Details: Interface Details section contains:

Section	Description
Configuration Information	Interface type, speed, and MTU. For SCTP links, this section also provides the IP address, mask, and physical address.
Status Information	Length of time the interface is up, administrative and operational status, and status of the line protocol.
Statistics Information	Number of bytes and packets that have been received and transmitted on the interface.
Errors Information	Number of packet errors and discarded packets.

Configuration Information

The Configuration Information subsection in the Statistics Details: Interface Details section for application server process associations, links, and signaling gateway mated pairs contains:

Field	Description
Type	Type of interface, such as Ethernet.
MTU	Size, in bytes, of the largest datagram that can send or receive on the interface.
Speed (Bits/Sec)	Estimate, in bits per second, of the interface's current bandwidth. If the interface does not vary in bandwidth; or, if no accurate estimate can be made, this field displays the nominal bandwidth.
IP Address	(SCTP links only) IP address corresponding to the media-dependent physical address. If the interface does not have such an address (for example, a serial line), this field displays N/A.
IP Mask	(SCTP links only) Subnet mask corresponding to the media-dependent physical address. If the interface does not have such an address (for example, a serial line), this field displays N/A.
Physical Address	(SCTP links only) Address of the interface at the protocol layer immediately below the network layer in the protocol stack. If the interface does not have such an address (for example, a serial line), this field displays N/A.



Note

This section does not appear if the application server process association, link, or signaling gateway mated pair has been offloaded to a Service and Application Module for IP () card.

Status Information

The Status Information subsection in the Statistics Details: Interface Details section for application server process associations, links, and signaling gateway mated pairs contains:

Field	Description
Uptime	Time the interface is up, in days, hours, minutes, and seconds.
Admin Status	State of the interface. Possible values are: - Up - Down - Testing
Operational Status	Current operational state of the interface. Possible values are: - Up - Down - Testing - Unknown - Dormant
Line Protocol Status	Current state of the line protocol. Possible values are: Up—Software processes that handle the line protocol consider the line to be usable (that is, keepalives are successful). Down—Software processes that handle the line protocol consider the line to be unusable. You can use the Line Protocol together with Operational Status to troubleshoot interface connection problems. For example, if Operational Status is Up, but Line Protocol is Down, the interface has detected a carrier on the physical layer, but clocking or framing problems might occur.

Statistics Information

The Statistics Information subsection in the Statistics Details: Interface Details section for application server process associations, links, and signaling gateway mated pairs contains:

Field	Description
Bytes In per Sec	Number of bytes received on the interface per second, including framing characters.
Bytes Out per Sec	Number of bytes sent on the interface per second, including framing characters.
Packets In per Sec	Number of packets delivered per second to a higher-layer protocol.
Packets Out per Sec	Total number of packets that higher-level protocols requested to be sent to the network per second, including those that were discarded or not sent.

Errors Information

The Errors Information subsection in the Statistics Details: Interface Details section for application server process associations, links, and signaling gateway mated pairs contains:

Field	Description
In Discards	Number of inbound packets that were discarded, even though no errors were detected to prevent their delivery to a higher-layer protocol. For example, a packet might be discarded to free buffer space.
Out Discards	Number of outbound packets that were discarded, even though no errors were detected to prevent their delivery to a higher-layer protocol. For example, a packet might be discarded to free buffer space.
In Errors	Number of inbound packets that contained errors that prevented their delivery to a higher-layer protocol.
Out Errors	Number of outbound packets that were not sent because of errors.

Poll Settings

To view or change poll settings for the object's Statistics Details window in the MWTM client interface, click **Poll Settings** in the left pane. The MWTM displays the Poll Settings pane in the right pane.

The Poll Settings pane contains:

Field	Description
Poll Interval (secs)	New poll interval for the object's Statistics Details window, in seconds. Enter the new poll interval in this field. The valid range is 15 seconds to an unlimited number of seconds. The default value is 15 seconds.
Current Poll Interval	Current poll interval for the object's Statistics Details window, in seconds.
Number of Polls Received	Total number of polls received since polling began for the object's Statistics Details window.
Running Time	Total elapsed time since polling began for the object's Statistics Details window.
Last Message	Date and time of the last poll for the object's Statistics Details window.
Poll Counter Mode	Displays the current mode for poll counters, and the date and time that counters were last reset. Possible modes are: • Since Reboot—Counters display values aggregated since the last reboot of the node, or since the node last reset the counters. • Since Last Poll—Counters display values aggregated since the last poll. • Since User Reset—Counters display values aggregated since the last time they were reset by the user.
Reset Counters	Opens the MWTM Reset Counters dialog box, which you use to change MWTM poller and counter settings. For more information, see Changing Real-Time Poller and Counter Settings, page 5-21 .

Q.752 Measurements

The Statistics Details: Q.752 Measurements section for links contains:

- [Error Information, page 8-76](#)
- [Inhibited Information, page 8-76](#)
- [Retransmitted Information, page 8-76](#)
- [Congested Information, page 8-77](#)

Statistics for links associated with the chosen linkset are visible in the left column, and for links associated with the adjacent linkset in the right column.

Error Information

The Error Information subsection contains:

Field	Description
Link Failure Count	Number of times the link was unavailable for signaling.
Alignment Error Count	Number of errors detected during link alignment. Link alignment occurs at start up, or when trying to bring up a failed link.
Negative ACKs Count	Number of errors detected during link acknowledgement.
Status Indicator Busy Count	Number of times the Status Indicator Busy was received.

Inhibited Information

The Inhibited Information subsection contains:

Field	Description
Local Inhibit Onset	Number of times a local ITP administrator has inhibited the link (that is, set the link to prevent traffic from flowing).
Local Inhibit Duration %	Percentage of time the link is locally inhibited since the last reboot of the ITP, or since ITP last reset the counters.
Remote Inhibit Onset	Number of times a remote ITP administrator has inhibited the link.
Remote Inhibit Duration %	Percentage of time the link is remotely inhibited since the last reboot of the ITP, or since ITP last reset the counters.

Retransmitted Information

The Retransmitted Information subsection contains:

Field	Description
Packets Retransmitted per Sec	Number of packets that the link transmits, per second.
Bytes Retransmitted per Sec	Number of bytes that the link transmits, per second.

Field	Description
Local Automatic Change Over Count	Number of <i>local automatic changeover</i> events detected.
Local Automatic Change Back Count	Number of <i>local automatic changeback</i> events detected.

Congested Information

The Congested Information subsection contains:

Field or Column	Description
Congestion Occurrences	Number of times congestion has occurred on the link.
Congestion Duration %	Percentage of time the link is congested since the last reboot of the ITP, or since ITP last reset the counters.
Congestion Level	Level of congestion: 1, 2, or 3.
Packets Lost	Number of packets lost by the link as a result of congestion at each level.
Packets Lost per Sec	Number of packets per second that the link loses, as a result of congestion at each level.
Times At Level With Packet Loss	Number of times the link is congested and has lost packets at each level.

Right-Click Menu

The Statistics Details window for a link in the MWTM client interface provides a right-click menu. To see this menu, right-click a link in the navigation tree of the Statistics Details window. The menu displays:

Menu Command	Description
Delete Item	Deletes the currently chosen link from the MWTM database. The MWTM displays the Confirm Deletion dialog box, To: - Delete the chosen link, click Yes. The MWTM deletes the link from the MWTM database and closes the Confirm Deletion dialog box. - Retain the chosen link, click No. The MWTM retains the link in the MWTM database and closes the Confirm Deletion dialog box. - Prevent the MWTM from displaying the Confirm Deletion dialog box, check the Do not show this again check box. Note If you check the Do not show this again check box, and you later decide you want the MWTM to begin displaying the Confirm Deletion dialog box again, you must check the Confirm Deletions check box in the General GUI settings in the Preferences window. For more information, see the description of the Confirm Deletions check box in Startup/Exit Settings, page 5-4. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.
Ignore Item	Ignores the link that you click at the next polling cycle. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.
Unignore Item	Stops ignoring the chosen link at the next polling cycle. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Power User (level 2) and higher.

SCTP Association Configuration Details

You use the MWTM to view Stream Control Transmission Protocol (SCTP) association configuration details for the chosen application server process association, link, or signaling gateway-mated pair.

The Statistics Details: SCTP Assoc. Config Details section contains:

Section	Description
Configuration Information	Status information, length of time the link is up, remote and local numbers, and IP address information.
Local IP Address Information	Local IP addresses associated with the link and the length of time each address is up.

Section	Description
Remote IP Address Information	Remote IP addresses associated with the link, the length of time each address is up, and SCTP retry information.
Transmission Configuration Information	The MTU, number of inbound and outbound streams, retry timeouts, local and remote receive window sizes, and chunk bundling information.

Configuration Information

The Configuration Information subsection in the Statistics Details: SCTP Assoc. Config Details section for application server process associations, SCTP links, and signaling gateway mated pairs contains:

Field	Description
Status	Current status of the SCTP association. Possible values are: - Closed - CookieWait - CookieEchoed
Status (continued)	- DeleteTCB - Established
Status (continued)	- ShutdownAckSent - ShutdownPending - ShutdownReceived - ShutdownSent For detailed information about each status, refer to RFC 2960, Stream Control Transmission Protocol.
Uptime	Time the link is up, in days, hours, minutes, and seconds.
Remote Port	Remote port number for the SCTP association.
Local Port	Local port number for the SCTP association.
Primary IP Address	Designated primary IP address for the SCTP association.
Effective IP Address	IP address that the SCTP association uses.

Local IP Address Information

The Local IP Address Information subsection in the Statistics Details: SCTP Assoc. Config Details section for application server process associations, SCTP links, and signaling gateway mated pairs contains:

Field	Description
IP Address	Local IP addresses associated with the link.
Uptime	Time each local IP address associated with the link is up, in days, hours, minutes, and seconds.

Remote IP Address Information

The Remote IP Address Information subsection in the Statistics Details: SCTP Assoc. Config Details section for application server process associations, SCTP links, and signaling gateway mated pairs contains:

Field	Description
IP Address	Remote IP addresses associated with the link.
Uptime	Time each remote IP address associated with the link is up, in days, hours, minutes, and seconds.
Retry Timeout (msecs)	Current SCTP Retransmission Timeout (T3-rtx timer).
Maximum Retries	Maximum allowable number of retransmissions before this IP address is considered inactive.
Retries	Current retransmission count.

Transmission Configuration Information

The Transmission Configuration Information subsection contains:

Field	Description
MTU	Maximum transmission unit (MTU) size that this SCTP association uses. Out of the IP addresses that the SCTP association uses, the smallest size that is supported.
In Streams	Inbound streams as negotiated when the SCTP association was started.
Out Streams	Outbound streams as negotiated when the SCTP association was started.
Maximum Retries	Maximum number of data retransmissions in the SCTP association context.
Local Receive window Size	Current local receive window size for this SCTP association.
Remote Receive window Size	Current local send window size for this SCTP association.
Initial Retry Timeout (msecs)	Initial timeout value, in milliseconds, that the SCTP implementation permits for the retry timeout.
Minimum Retry Timeout (msecs)	Minimum timeout value, in milliseconds, that the SCTP implementation permits for the retry timeout.
Maximum Retry Timeout (msecs)	Maximum timeout value, in milliseconds, that the SCTP implementation permits for the retry timeout.
Bundle Chunks	Indicates whether the SCTP protocol allows chunks to be bundled into a single datagram as follows. Valid values are: true (1)—Chunks are bundled. false (2)—Chunks are not bundled.
Bundle Timeout (msecs)	Time, in milliseconds, to wait to allow data chunks to accumulate so that they can be transmitted in the same datagram.

SCTP Association Statistics Details

You use the MWTM to view Stream Control Transmission Protocol (SCTP) association statistics details for the chosen application server process association, link, or signaling gateway-mated pair.

The Statistics Details: SCTP Assoc. Stats Details section contains:

Section	Description
Remote IP Address Information	IP addresses, round-trip times, failure counts, and IP address status and heartbeat.
Statistics Information (per sec) Rates	Sent and received counts for packets and chunks.

Remote IP Address Information

The Remote IP Address Information subsection in the Statistics Details: SCTP Assoc. Stats Details section for application server process associations, SCTP links, and signaling gateway mated pairs contains:

Field	Description
IP Address	Remote IP addresses associated with the link.
Smoothed Round Trip Time (msecs)	Average, in milliseconds, of all round-trip times between the local and remote systems on an IP network.
Failure Count	Number of times the remote IP address was marked as failed.
Heartbeat Status	Current status of the heartbeat associated with the remote IP address. Valid values are Active and Inactive.
IP Status	Current status of the remote IP address. Valid values are Active and Inactive.

Statistics Information (per sec) Rates

The Statistics Information (per sec) Rates subsection in the Statistics Details: SCTP Assoc. Stats Details section for application server process associations, SCTP links, and signaling gateway mated pairs contains:

Field	Description
Packets Sent	Number of IP datagrams that this SCTP association sends per second.
Packets Received	Number of IP datagrams that this SCTP association receives per second.
Control Chunks Sent	Number of control chunks that this SCTP association sends per second.
Control Chunks Rec	Number of control chunks that this SCTP association receives per second.
Ordered Chunks Sent	Number of ordered chunks that this SCTP association sends per second.
Ordered Chunks Rec	Number of ordered chunks that this SCTP association receives per second.
Unordered Chunks Sent	Number of unordered chunks that this SCTP association sends per second.

Field	Description
Unordered Chunks Rec	Number of unordered chunks that this SCTP association receives per second.
Retransmitted Chunks	Number of chunks that this SCTP association retransmits per second.
Retransmitted Fast Chunks	Number of fast chunks that this SCTP association retransmits per second.

Statistics: Application Servers

You use the MWTM to view statistics for a chosen application server.

The Statistics Details: Statistics tab contains:

Field	Description
Active Duration	Total time the application server is in service since the last reboot of the ITP, or since ITP last reset the counters.
MTP3 Packet Rate (per sec)	Number of MTP3 packets that the application server receives per second. This field initially displays the description <code>Waiting for second poll</code> . After two polling cycles, the MWTM populates this field with actual calculated rates.
ASP Packet Rate (per sec)	Number of application server process packets that the application server sends per second. This field initially displays the description <code>Waiting for second poll</code> . After two polling cycles, the MWTM populates this field with actual calculated rates.

Statistics: Application Server Process Associations

You use the MWTM to view statistics for a chosen application server process association.

The Statistics Details: Statistics tab contains:

- [Packets Per Second Information, page 8-83](#)
- [Error Information, page 8-83](#)
- [ASP Initialization Counters, page 8-83](#)
- [Signaling Congestion Counters, page 8-84](#)
- [Destination Counters, page 8-84](#)

Packets Per Second Information

The Packets Per Second Information section in the Statistics Details: Statistics tab for application server process associations contains:

Field	Description
Packets From ASP	Number of packets that the application server receives per second.
Packets To ASP	Number of packets that the application server sends per second.
Packets From MTP3	Number of packets that the MTP3 layer receives per second.
Packets To MTP3	Number of packets that the MTP3 layer sends per second.

Error Information

The Error Information section in the Statistics Details: Statistics tab for application server process associations contains:

Field	Description
Errors Received	Total number of error (ERR) messages that the application server process association receives.
Errors Sent	Total number of error (ERR) messages that the application server process association sends.

ASP Initialization Counters

The ASP Initialization Counters section in the Statistics Details: Statistics tab for application server process associations contains:

Field	Description
Up Messages Received	Total number of application server process up (ASPUP) messages that the application server process association receives.
Up ACK Messages Sent	Total number of application server process up acknowledgement (UPACK) messages that the application server process association sends.
Down Messages Received	Total number of application server process down (ASPDN) messages that the application server process receives.
Down ACK Messages Sent	Total number of application server process down acknowledgement (DOWNACK) messages that the application server process association sends.
Activation Messages Received	Total number of application server process active messages that the application server process association receives.
Activation ACK Messages Sent	Total number of application server process active acknowledgement messages that the application server process association sends.

Field	Description
Inactive Messages Received	Total number of application server process inactive messages that the application server process association receives.
Inactive ACK Messages Sent	Total number of application server process inactive acknowledgement messages that the application server process association sends.

Signaling Congestion Counters

The Signaling Congestion Counters section in the Statistics Details: Statistics tab for application server process associations contains:

Field	Description
Level 0 Messages Received	Total number of signaling congestion level 0 (SCON0) messages that the application server process receives.
Level 1 Messages Received	Total number of signaling congestion level 1 (SCON1) messages that the application server process receives.
Level 2 Messages Received	Total number of signaling congestion level 2 (SCON2) messages that the application server process receives.
Level 3 Messages Received	Total number of signaling congestion level 3 (SCON3) messages that the application server process receives.
Level 0 Messages Sent	Total number of signaling congestion level 0 (SCON0) messages that the application server process sends.
Level 1 Messages Sent	Total number of signaling congestion level 1 (SCON1) messages that the application server process sends.
Level 2 Messages Sent	Total number of signaling congestion level 2 (SCON2) messages that the application server process sends.
Level 3 Messages Sent	Total number of signaling congestion level 3 (SCON3) messages that the application server process sends.

Destination Counters

The Destination Counters section in the Statistics Details: Statistics tab for application server process associations contains:

Field	Description
Unavailable Messages Received	Total number of destination unavailable (DUNA) messages that the application server process association receives.
Unavailable Messages Sent	Total number of destination unavailable (DUNA) messages that the application server process association sends.
Available Messages Received	Total number of destination available (DAVA) messages that the application server process association receives.
Available Messages Sent	Total number of destination available (DAVA) messages that the application server process association sends.

Field	Description
User Part Unavailable Messages Received	Total number of destination user part unavailable (DUPU) messages that the application server process association receives.
User Part Unavailable Messages Sent	Total number of destination user part unavailable (DUPU) messages that the application server process association sends.
State Audit Messages Received	Total number of destination state audit (DAUD) messages that the application server process association receives.
State Audit Messages Sent	Total number of destination state audit (DAUD) messages that the application server process association sends.

Statistics: Links and Linksets

You use the MWTM to view statistics for a chosen link or linkset.

The Statistics Details: Statistics tab contains:

- [Packet Information, page 8-85](#)
- [Bit Information or Byte Information, page 8-86](#)
- [LSSU Information \(Links Only\), page 8-86](#)
- [Utilization Information, page 8-87](#)
- [Service Information, page 8-88](#)

Statistics for links associated with the chosen linkset are visible in the left column, and for links associated with the adjacent linkset in the right column.

Packet Information

The Packet Information section in the Statistics Details: Statistics tab for links and linksets contains:

Field	Description
Sent Per Sec	Number of packets that the link or linkset sends per second. This field initially displays the description <code>Waiting for second poll</code> . After two polling cycles, the MWTM populates this field with actual calculated rates.
Received Per Sec	Number of packets that the link or linkset receives per second. This field initially displays the description <code>Waiting for second poll</code> . After two polling cycles, the MWTM populates this field with actual calculated rates.
Drops	Total number of packets that have been dropped by the link or linkset.
Transmit Queue Depth (links only)	Number of packets waiting to be sent on by the link.
Transmit Queue High Depth (links only)	Highest level reached by the transmit queue since the last reboot of the ITP, or since ITP last reset the averages as a result of bad data.

Field	Description
Transmit Queue High Reset (links only)	Level at which the link is to reset the transmit queue. If the link is never to reset the transmit queue, this field displays <i>Never</i> .
Signal Link Test (links only)	Indicates whether test packets are being sent on the link. Valid values are: true (1)—Test packets are being sent. false (2)—Test packets are not being sent.

Bit Information or Byte Information

The Bit Information section (or Byte Information section, if you unchecked the Show Details in Bits Instead of Bytes check box in the Preferences window) in the Statistics Details: Statistics tab for links and linksets contains these fields:

Field	Description
Sent Per Sec	Number of bits or bytes (as set in the Preferences window) that the link or linkset sends per second. This field initially displays the description <i>waiting for second poll</i> . After two polling cycles, the MWTM populates this field with actual calculated rates.
Received Per Sec	Number of bits or bytes (as set in the Preferences window) that the link or linkset receives per second. This field initially displays the description <i>waiting for second poll</i> . After two polling cycles, the MWTM populates this field with actual calculated rates.

LSSU Information (Links Only)

The Links Status Signal Unit (LSSU) section in the Statistics Details: Statistics tab for links contains:

Field	Description
LSSU Packets Sent	Total number of LSSU packets that the link sends.
LSSU Packets Received	Total number of SS7 Message Transfer Part Layer 2 (MTP2) LSSU packets that the link receives.

Utilization Information

The Utilization Information section in the Statistics Details: Statistics tab for links and linksets contains:

Field	Description
Send Plan Capacity	Planned capacity of the link or linkset to send, in bits per second. For a link or linkset of type: - Serial or HSL, available bandwidth for the link/linkset. - SCTPIP (or Mixed for linksets), set on the ITP by using the plan-capacity CS7 link or linkset configuration command. If Send Plan Capacity is not set on the ITP for this link or linkset, this field displays the value 0. - Other, this field always displays the value 0.
%	Amount of the link or linkset's send capacity being used, as a percentage or in Erlangs (E) as set in the Preferences window, calculated by using this formula: $\text{Send Utilization} = (\text{Bits Sent Per Sec}) / \text{Planned Capacity}$
% (continued)	This field initially displays the description <code>Waiting for second poll</code> . After two polling cycles, the MWTM populates this field with actual calculated rates. For a link or linkset of type: - SCTPIP (or Mixed for linksets), if Send Plan Capacity is not set on the ITP for this link, or for one or more of the links associated with this linkset, this field displays the description <code>Set Plan Capacity on ITP</code>. - Other, this field always displays the description <code>Set Plan Capacity on ITP</code>.
Send Threshold % (links only)	Indicates when to generate the MWTM a cItpSpLinkSentUtilChange for the link, as a percent of its total send capacity. For example, if Send Plan Capacity is 64,000 bits per second, and Send Threshold % is 50 , then the MWTM generates a cItpSpLinkSentUtilChange notification when the link reaches 50% of 64,000, or 32,000 bits per second.
Receive Plan Capacity	Planned capacity of the link or linkset to receive, in bits per second. For a link or linkset of type: - Serial or HSL, available bandwidth for the link. - SCTPIP (or Mixed for linksets), set on the ITP using the plan-capacity CS7 link/linkset configuration command. If Receive Plan Capacity is not set on the ITP for this link or linkset, this field displays the value 0. - Other, this field always displays the value 0.

Field	Description
Receive Utilization %	Amount of the link or linksets receive capacity being used, as a percentage or in Erlangs (E) as set in the Preferences window, calculated by using this formula: $\text{Receive Utilization} = (\text{Bits Received Per Sec}) / \text{Receive Plan Capacity}$ This field initially displays the description <code>Waiting for second poll</code>. After two polling cycles, the MWTM populates this field with actual calculated rates. For a link or linkset of type: - SCTPIP (or Mixed for linksets), if Receive Plan Capacity is not set on the ITP for this link, or for one or more of the links associated with this linkset, this field displays the description <code>Set Plan Capacity on ITP</code>. - Other, this field always displays the description <code>Set Plan Capacity on ITP</code>.
Receive Threshold % (links only)	Indicates when to generate the MWTM a <code>cltpSpLinkRcvdUtilChange</code> for the link, as a percent of its total receive capacity. For example, if Receive Plan Capacity is 64,000 bits per second, and Receive Threshold % is 50, then the MWTM generates a <code>cltpSpLinkRcvdUtilChange</code> notification when the link reaches 50% of 64,000, or 32,000 bits per second.

Service Information

The Service Information section in the Statistics Details: Statistics tab for links and linksets contains:

Field	Description
Duration In Service %	Percentage of time the link or linkset is in service since the last reboot of the ITP, or since ITP last reset the counters.
Duration Out Of Service %	Percentage of time the link or linkset is out of service since the last reboot of the ITP, or since ITP last reset the counters.
MTP3 Accounting Enabled (linksets only)	Indicates whether the collection of MTP3 accounting statistics is enabled for the linkset. If the linkset is a Virtual linkset, this field displays N/A.
GTT Accounting Enabled (linksets only)	Indicates whether the collection of GTT accounting statistics is enabled for the linkset. For Cisco IOS software releases prior to 12.2(4)MB10, this field displays Unknown. If the linkset is a Virtual linkset, this field displays N/A.

Status Details

You use the MWTM to view status details for a chosen link.

The Statistics Details: Status Details tab contains:

Column	Description
Protocol State Details	Detailed information about the state of the protocol for this link. Possible values are: • Changeback control (TCBC)—Changeback control is buffering data on this link. • Changeover control (TCOC)—Changeover control is buffering data on this link. • Link availability control (TLAC)—Adjacent Signalling point is restarting. • Link availability control (TLAC)—Emergency changeover is in progress on this link. • Link availability control (TLAC)—Changeback is in progress on this link. • Link availability control (TLAC)—Changeover is in progress on this link. • Link availability control (TLAC)—The last changeover operation failed on this link. • Link availability control (TLAC)—Inhibit command will be retried.
Protocol State Details (continued)	• Link availability control (TLAC)—Management request in progress for this link. • Link availability control (TLAC)—Signalling point is in the process of a restart. • Signalling routing control (TSRC)—Changeover request is complete. • Signalling routing control (TSRC)—Adjacent Signalling Point is restarting. • Link availability control (TLAC)—Link is inhibited by a local management operation. • Link availability control (TLAC)—Link is inhibited by a remote management operation. • Link availability control (TLAC)—Link is blocked because of a local processor outage. • Link availability control (TLAC)—Link is blocked because of a remote processor outage.

Column	Description
Link Test Results	Indicates the results of the link test. Possible results are: • No Errors—The link did not detect any errors. • Undefined OPC (Origination Point Code)—A signaling link test message arrived with an undefined OPC. This scenario can occur when a serial link connects incorrectly, or when you configure an SCTP link incorrectly. This scenario differs from Incorrect OPC because the signaling point is unaware of the point code in question. The point code is not defined for any linkset on this ITP. • Incorrect OPC—A signaling link test message arrived with an incorrect OPC. This scenario can occur when a serial link connects incorrectly, or when you configure an SCTP link incorrectly. This scenario differs from Undefined OPC because the signaling point is aware of the point code in question, and the point code is defined for a linkset on this ITP, but the point code is not correct for the current linkset. • Undefined SLC (Signaling Link Code)—A signaling link test message arrived with an undefined SLC. This scenario can occur when a serial link connects incorrectly, or when you configure an SCTP link incorrectly. The link connects to the correct linkset, but the linkset does not have a definition for the SLC in question. • Incorrect SLC—A signaling link test message arrived with an incorrect SLC. This scenario can occur when a serial link connects incorrectly, or when you configure an SCTP link incorrectly. The link connects to the correct linkset, but to the wrong link in that linkset. That is, the signaling test receives the test packet on the wrong link.
Link Test Results (continued)	• Incorrect NI (Network Indicator)—A signaling link test message arrived with an incorrect NI. This scenario can occur when links connect to the correct linkset and link, but the NIs of the two adjacent point codes are not the same. • Bad Pattern—A signaling link test message arrived with an incorrect test pattern. This error occurs because the test pattern is corrupt. This scenario usually indicates a hardware or configuration issue related to the physical format of the data on the links, caused by a variant mismatch or incorrect definitions on the physical link. • Non Adjacent—Received a signaling link test message from a nonadjacent node. • Failed—Unable to run the test, or no response arrived in the specified interval.

Column	Description
Link Fail Reason	If the link failed the link test, indicates the reason for the failure. Possible reasons are: • None—No additional reason available. • Changeover in progress—Changeover is in progress. This message diverts traffic away from a failed link. • Management disconnect request—An MTP3 sent a request to stop the link. • Link alignment lost—Link alignment is lost. A link is in alignment when signal units are received in sequence, and with the proper number of octets. The signal unit must be a total length of eight-bit multiples. If the signal unit is not of eight-bit multiples, or if the signaling information field (SIF) exceeds the 272-octet capacity, the signaling unit is considered to be in error. If excessive errors are encountered on a link, it is considered to be out of alignment. For M2PA links, this state reason is generated when the M2PA alignment timer T1 expires. This could indicate that the remote link is shutdown, or that intermittent IP connectivity problems exist. • Link connection lost—Link connection is lost. • Local Disconnect—A request to disconnect the link is received, but the link is already disconnected. • Remote Disconnect—A remote disconnect request is received. • Signal unit error rate monitor failure—The signal unit error rate monitor has failed. • T1 timeout no FISU received—A T1 timeout no FISU is received. This timer avoids message mis-sequencing during changeover. • T2 timeout no SIO received—A T2 timeout no SIO is received. This timer waits for a changeover acknowledgment.

Column	Description
Link Fail Reason (continued)	• T3 timeout no SIN received—A T3 timeout no SIN is received. This timer controls diversion-delay to avoid mis-sequencing on changeback. • T6 timeout excessive congestion—A T6 timeout excessive congestion is received. This timer avoids message mis-sequencing on controlled rerouting. • T7 timeout excessive acknowledgement delay—A T7 timeout excessive acknowledgment delay is received. The T7 timer prevents a signaling point from waiting too long for a positive or negative acknowledgment. Usually, an acknowledgment is sent when a signaling point becomes idle and does not have any more traffic to transmit. When congestion occurs at a signaling point, or an extreme amount of traffic is present, the T7 could possibly time out and force retransmission of messages. • Link proving failure—A link proving failure occurred. • Abnormal BSN received—An abnormal Backward Sequence Number (BSN) is received. • Abnormal FIB received—An abnormal Forward Indicator Bit (FIB) is received. • Abnormal SIB received—An abnormal Status Indicator Busy (SIB) is received. • Abnormal LSSU received—An abnormal Link Status Signal Unit (LSSU) is received. • Peer not ready—An MTP3 tried to bring up a link that is still cleaning up after being stopped. In some cases, the MTP3 does not change over after a link failure, so the M2PA or SCTP waits for an event that will not occur. When an MTP3 tries to bring up the link again, the previous control structures must first be cleaned up. If M2PA gets a start request from an MTP3, and the previous structures are still being held, M2PA cleans them up and sends a PEER NOT READY to the MTP3 layer. A subsequent request to start the link from the MTP3 layer will then cause the link to come up. • Communication lost—M2PA or SCTP has determined that the remote end signaling point is no longer reachable. Possible reasons include: – The maximum number of consecutive retries of a packet is reached. – In the absence of data, the MWTM failed to receive heartbeat ACKs in response to heartbeats, for the maximum number of retries. • No Listen posted—An MTP3 tried to start a link, but the local-peer port associated with the link is not available, probably because of a bad configuration. • Unable to allocate buffer—M2PA or SCTP cannot get buffers for sending or receiving packets. Buffer problems can be temporary or permanent. Temporary buffer problems will generally clear with little side effects. Permanent buffer problems can lead to failed linksets or links.

Column	Description
Link Fail Reason (continued)	• Link card removed—A link card is removed. • Link card inserted—A link card is inserted. • False link congestion—A false link congestion indication is received. • Configuration downloading—The configuration is downloading. • Locally inhibited—The link is locally inhibited by operator request. • Locally uninhibited—An operator request locally uninhibited the link. • Remotely inhibited—The link is remotely inhibited by operator request. • Remotely uninhibited—The link is remotely uninhibited by operator request. • Locally blocked—The link is blocked locally. • Locally unblocked—The link is unblocked locally. • Remotely blocked—The link is remotely blocked. • Remotely unblocked—The link is remotely unblocked.

Viewing ITP MTP3 Errors

The ITP MTP3 Errors table displays all MTP3 error information for the chosen ITP node.

If you have implemented MWTM User-Based Access, this option is available to users with authentication level System Administrator (level 5).



Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

The MTP3 Errors section displays these columns for the chosen node:

Column	Description
Reset Counters	Opens the MWTM Reset Counters dialog box, which you use to change MWTM poller and counter settings. For more information, see Changing Real-Time Poller and Counter Settings, page 5-21 .
Poll Counter Mode	Displays the current mode for poll counters, and the date and time that counters were last reset. Possible modes are: • Since Reboot—Counters display values aggregated since the last reboot of the ITP, or since ITP last reset the counters. • Since Last Poll—Counters display values aggregated since the last poll. • Since User Reset—Counters display values aggregated since the last time they were reset by the user.
Poll Interval	Poll interval used to collect data for the table.

Column	Description
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Count	Number of times the indicated MTP3 error type was detected.
Error Description	Description of the MTP3 error type.

Viewing ITP MSU Rates

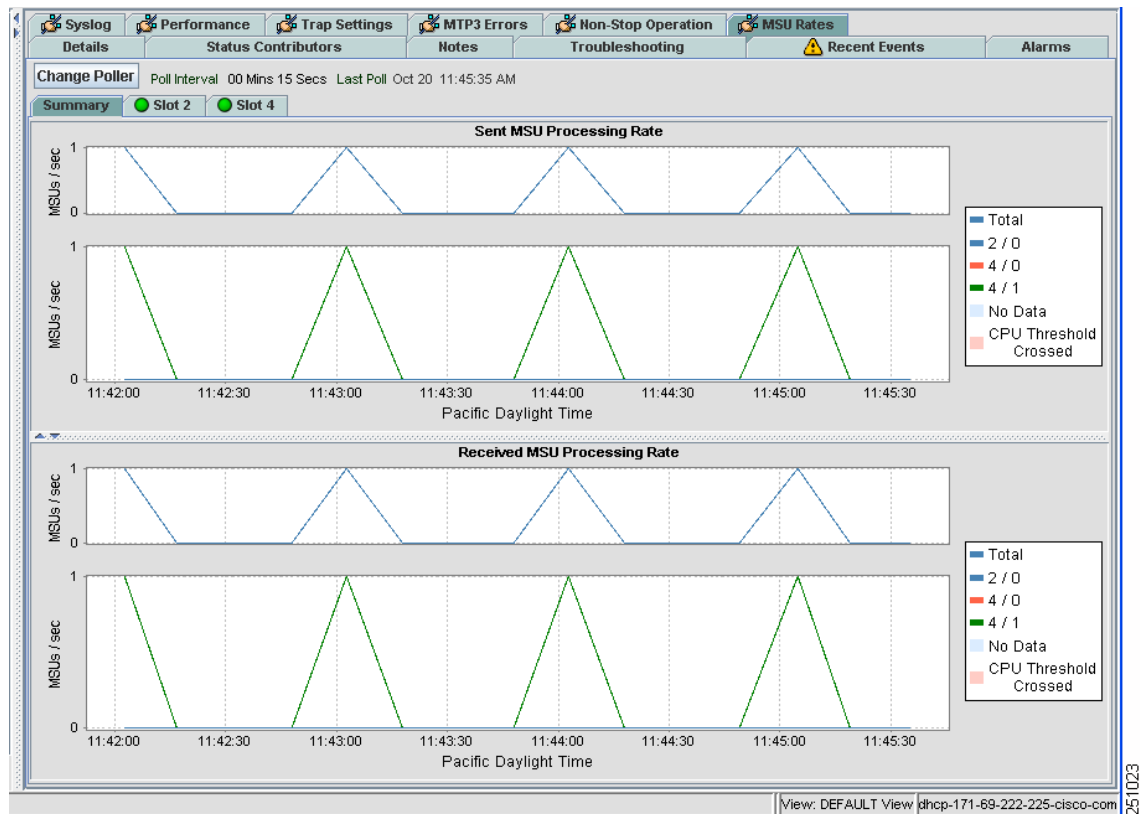
The ITP MSU Rates table displays all MSU rate information in charts for the chosen ITP node.



Note

In the MWTM client, the real-time icon appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

Figure 8-4 MSU Rates Tab



The MSU Rates tab contains a Summary sub-tab, showing totals for all MSU rates. Each additional sub-tab shows MSU rates for a specific CPU (for example, 0/0 shows CPU 0 located in slot 0). The status ball on the sub-tab indicates the current threshold level of the CPU.

GUI Elements	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Poll Interval	Label that shows the current poll interval in seconds.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
MSUs / sec	Y-axis label that displays traffic rate in MSUs per second.
Time	X-axis label that displays a real-time scale.
Legend	Identifies the data series currently showing in the chart. • No Data—Data is not available. A vertical bar appears in the chart. • CPU Threshold Crossed—One or more CPUs have crossed a processing threshold.

Right-click Menu

A right-click context menu provides options to modify how the chart appears:

Menu options	Description
Hide > <i>field</i>	Hides the currently shown data series.
Show > <i>field</i>	Shows the currently shown data series.
Reset Zoom	If you have zoomed into a specific area of the chart, resets the zoom. Note To zoom into a specific area of the chart, use the left mouse button to drag a box around the area.
Grid On	Displays a grid on the chart.
Grid Off	Removes the grid from the chart.
Shapes On	Displays individual data points as shapes on the rate lines and the chart legend.
Shapes Off	Removes shapes from the rate lines and the chart legend.

Viewing ITP Non-Stop Operation

Non-Stop Operation (NSO) is an implementation of redundant data elements and software functionality that enables networks to approach 99.999% availability. The ITP Non-Stop Operation table displays detailed information about all NSO settings associated with the chosen node.

To view the Non-Stop Operation section, in a view in the navigation tree, select an ITP node, then click on the Non-Stop Operation tab in the content area. This tab appears only for Cisco 7500 and Cisco 7600 nodes.



Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

The Non-Stop Operation table displays these columns for the chosen node:

Column	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Configuration: Split Mode	Indicates whether redundant units can communicate synchronization messages with each other: • Enabled—Communication is not permitted. The active unit does not communicate with the standby unit, and the standby unit progression does not occur. This mode can be useful during maintenance. • Disabled—Communication is permitted. The active unit communicates with the standby unit, and the standby unit is reset to recover.
Configuration: Keepalive Threshold	On platforms that support keepalives, this field indicates the number of lost keepalives allowed before a failure occurs. If a failure occurs, a Switch of Activity (SWACT) notification switches the active unit to standby status, and vice versa. On platforms that do not support keepalives, this field has no meaning.
Configuration: Keepalive Threshold Min	Minimum acceptable value for the Keepalive Threshold.
Configuration: Keepalive Threshold Max	Maximum acceptable value for the Keepalive Threshold.
Configuration: Keepalive Timer (msecs)	On platforms that support keepalives, this timer guards against lost keepalives. If the RF subsystem does not receive a keepalive before this timer expires, a SWACT notification switches the active unit to standby status, and vice versa. On platforms that do not support keepalives, this field has no meaning.
Configuration: Keepalive Time Min (msecs)	Minimum acceptable value for the Keepalive Timer.
Configuration: Keepalive Time Max (msecs)	Maximum acceptable value for the Keepalive Timer.

Column	Description
Configuration: Notification Timer (msecs)	RF notification timer. As the standby unit progresses to the Hot Standby state, the active unit sends asynchronous messages to the standby unit, which then sends an acknowledgment back to the active unit. If the active unit: • Receives the acknowledgement before this timer expires, the standby unit progresses normally. • Does not receive a acknowledgement before this timer expires, a SWACT notification switches the active unit to standby status, and vice versa.
Configuration: Notification Timer Min (msecs)	Minimum acceptable value for the Notification Timer.
Configuration: Notification Timer Max (msecs)	Maximum acceptable value for the Notification Timer.
Configuration: RF Notification	Indicates whether RF system notification is enabled or disabled.
Configuration: Maintenance Mode	Indicates whether the redundant system is in maintenance mode: • Enabled—The redundant system is in maintenance mode. The active unit does not communicate with the standby unit, and the standby unit progression does not occur. • Disabled—The redundant system is in normal operation mode, not maintenance mode. The active unit communicates with the standby unit, and the standby unit is reset to recover.

Column	Description
Configuration: Redundancy Mode	Redundancy mode configured on this system. Possible values are: • Cold Standby Redundant—This system is configured for redundancy, but the redundant peer unit is not fully initialized and cannot retain established calls. • Dynamic Load Share NonRedundant—This system is not configured for redundancy, but it is load-sharing. The load-sharing is based on the operational load (that is, it is based on the number of calls, or some other factor). • Static Load Share Redundant—This system is configured for redundancy, and it is load-sharing. The load-sharing is based on the operational load. • NonRedundant—This system is not configured for redundancy, and it is not load-sharing. • Static Load Share NonRedundant—This system is not configured for redundancy, but it is load-sharing. The load-sharing is not based on the operational load. • Static Load Share Redundant—This system is configured for redundancy, and it is load-sharing. The load-sharing is not based on the operational load. • Warm Standby Redundant—This system is configured for redundancy, and the redundant peer unit can immediately handle new calls, but it cannot retain established calls. • Hot Standby Redundant—This system is configured for redundancy, the redundant peer unit can immediately handle new calls, and it can <i>instantaneously</i> retain established calls.
Configuration: Redundancy Mode Descr	Additional clarification or description of the Redundancy Mode.
Configuration: Oper Redundancy Mode	Operational redundancy mode of this unit. Possible values are: • Cold Standby Redundant—This unit is configured for redundancy, but the redundant peer unit is not fully initialized and cannot retain established calls. • Dynamic Load Share NonRedundant—This unit is not configured for redundancy, but it is load-sharing. The load-sharing is based on the operational load (that is, it is based on the number of calls, or some other factor).

Column	Description
Configuration: Oper Redundancy Mode (continued)	• Static Load Share Redundant—This unit is configured for redundancy, and it is load-sharing. The load-sharing is based on the operational load. • NonRedundant—This unit is not configured for redundancy, and it is not load-sharing. • Static Load Share NonRedundant—This unit is not configured for redundancy, but it is load-sharing. The load-sharing is not based on the operational load. • Static Load Share Redundant—This unit is configured for redundancy, and it is load-sharing. The load-sharing is not based on the operational load. • Warm Standby Redundant—This unit is configured for redundancy, and the redundant peer unit can immediately handle new calls, but it cannot retain established calls. • Hot Standby Redundant—This unit is configured for redundancy, the redundant peer unit can immediately handle new calls, and it can <i>instantaneously</i> retain established calls.
History: Cold Starts	Number of system cold starts, including automatic and manual SWACTs, since the last system initialization.
History: Available Standby Time	Cumulative time that a standby redundant unit is available since the last system initialization.
Current Status: Unit ID	Unique identifier for this redundant unit.
Current Status: Unit State	Current RF status for this unit. Possible values are: • Active—Active and is processing calls. • Active Drain—Performing client cleanup. • Active Extra Load—Active and is processing calls for all feature boards in the system. • Active Fast—Performing call maintenance during a SWACT notification. • Active Handback—Active, is processing calls, and is handing off some resources to the other RF unit. • Active Preconfiguration—Active but has not yet read its configuration. • Active Postconfiguration—Active and is processing its configuration.

Column	Description
Current Status: Unit State (continued)	• Disabled—RF is not currently operating on this unit. • Hot Standby—Ready to become the active unit. • Initialization—Establishing necessary system services. • Negotiation—Discovering and negotiating with its peer unit. • Cold Standby—Running the client RF notification. • Cold Standby Bulk—Synchronizing its client data with the peer (active) unit. • Cold Standby Configuring—Synchronizing its configuration with the peer (active) unit. • Cold Standby File System—Synchronizing its file system with the “V unit”. • Unknown—The current RF state of this unit is not known.
Current Status: Peer Unit ID	Unique identifier for the peer redundant unit.
Current Status: Peer Unit State	Current RF status for this unit’s peer unit. Possible values are: • Active—Active and is processing calls. • Active Drain—Performing client cleanup. • Active Extra Load—Active and is processing calls for all feature boards in the system. • Active Fast—Performing call maintenance during a SWACT notification. • Active Handback—Active, is processing calls, and is handing off some resources to the other RF unit. • Active Preconfiguration—Active but has not yet read its configuration. • Active Postconfiguration—Active and is processing its configuration. • Disabled—RF is not currently operating on the peer unit. • Hot Standby—Ready to become the active unit. • Initialization—Establishing necessary system services. • Negotiation—Discovering and negotiating with this unit. • Cold Standby—Running the client RF notification. • Cold Standby Bulk—Synchronizing its client data with this (active) unit. • Cold Standby Configuring—Synchronizing its configuration with this (active) unit. • Cold Standby File System—Synchronizing its file system with this (active) unit. • Unknown—The current RF state of the peer unit is not known.

Column	Description
Current Status: Primary Mode	Indicates whether this unit is the primary or secondary. The primary unit has a higher priority than the secondary unit. In a race situation (for example, during initialization), or in any situation in which the units cannot successfully negotiate activity between themselves, the primary unit becomes the active unit and the secondary unit becomes the standby unit. Only one redundant unit can be the primary unit at any given time.
Current Status: Duplex Mode	Indicates whether the peer unit is detected: • Duplex—Detected. • Simplex—Not detected.
Current Status: Manual Switch Inhibit	Indicates whether a manual Switch of Activity (SWACT) is allowed: • Enabled—Not allowed. • Disabled—Allowed.
Current Status: Last Switchover Reason	Reason for the last Switch of Activity (SWACT). Possible values are: • Active Unit Failed—A failure of the active unit triggered an automatic SWACT. • Active Unit Removed—The removal of the active unit triggered an automatic SWACT. • None—No SWACT has occurred. • Unknown—The reason for the last SWACT is not known. • Unsupported—The reason code for the last SWACT is not supported. • User Forced—A user forced a manual SWACT, ignoring preconditions, warnings, and safety checks. • User Initiated—A user initiated a safe, manual SWACT.
Current Status: Total System Up Time	Date and time when this node was up.
Current Status: Last Failover Time	Date and time when the primary redundant unit became the active unit. If no failover has occurred, this field displays <code>No Failover Has Occurred</code> .
Current Status: Standby Available At Time	Date and time when the peer redundant unit entered the Hot Standby state. If a failover occurs, this field displays <code>System Initialization</code> for a brief period until the system is back up.

Column	Description
Redundancy Mode Capability: Capability Mode and Description	List of redundancy modes that the unit can support. Possible values are: • Cold Standby Redundant—This unit is configured for redundancy, but the redundant peer unit is not fully initialized and cannot retain established calls. • Dynamic Load Share NonRedundant—This unit is not configured for redundancy, but it is load-sharing. The load-sharing is based on the operational load (that is, it is based on the number of calls, or some other factor). • Static Load Share Redundant—This unit is configured for redundancy, and it is load-sharing. The load-sharing is based on the operational load. • NonRedundant—Redundancy is not configured on this unit, and it is not load-sharing. • Static Load Share NonRedundant—This unit is not configured for redundancy, but it is load-sharing. The load-sharing is not based on the operational load. • Static Load Share Redundant—This unit is configured for redundancy, and it is load-sharing. The load-sharing is not based on the operational load. • Warm Standby Redundant—This unit is configured for redundancy, and the redundant peer unit can immediately handle new calls, but it cannot retain established calls. • Hot Standby Redundant—This unit is configured for redundancy, the redundant peer unit can immediately handle new calls, and it can <i>instantaneously</i> retain established calls. The Description column contains additional clarification or description of the Capability Mode.
Switchover History: Index	Number identifying the entry in the Switchover History table.
Switchover History: Prev. ID	Unit ID of the active unit that failed or was removed.
Switchover History: Curr. ID	Unit ID of the standby unit that became the new active unit.
Switchover History: Reason	Reason for the SWACT. Possible values are: • Active Unit Failed—A failure of the active unit triggered an automatic SWACT. • Active Unit Removed—The removal of the active unit triggered an automatic SWACT. • None—No SWACT has occurred.

Column	Description
Switchover History: Reason (continued)	• Unknown—The reason for the last SWACT is not known. • Unsupported—The reason code for the last SWACT is not supported. • User Forced—A user forced a manual SWACT, ignoring preconditions, warnings, and safety checks. • User Initiated—A user initiated a safe, manual SWACT.
Switchover History: Time	Date and time that the SWACT occurred.

Viewing TDM Statistics

You can view real-time TDM statistics for T1 and E1 interfaces. To view TDM statistics for one of these interfaces, launch the MWTM client or MWTM web interface (<http://server name:1774>), select the T1 or E1 interface in the navigation tree (in the Physical folder), then click the TDM Statistics tab.



Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

The TDM Statistics tab contains:

GUI Element	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller , page 8-110. This button appears only in the MWTM client.
Poll Interval	Label that shows the current poll interval in seconds.
Last Poll	Label that identifies when the last poll occurred.
Line Configuration	Pane that lists the line configuration parameters of the chosen T1 or E1 interface. See Line Configuration Pane , page 8-103.
Line Status Information ¹	Pane that provides line status information for the chosen T1 or E1 interface. See Line Status Information Pane , page 8-106.
Performance / Error Information ¹	Pane that provides performance and error information for the chosen T1 or E1 interface. See Performance and Error Information Pane , page 8-106.

1. To run basic troubleshooting commands on T1 and E1 interfaces, click the Troubleshooting tab, and select the Layer 2 Cross Connection category. See [Viewing Troubleshooting](#), page 8-43.

Line Configuration Pane

The Line Configuration pane contains:

Parameter	Value
Interface Name	Name of the interface (for example, T1 0/0).
Line Type	Indicates the type of DS1 line that implements this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. Values include: • ESF—Extended Super Frame DS1. • D4—AT&T D4 format DS1. • E1—CCITT recommendation G.704 (Table 4a). • E1-CRC—CCITT recommendation G.704 (Table 4b). • E1-MF—G.704 (Table 4a) with TS16 multiframing enabled. • E1-CRC-MF—G.704 (Table 4b) with TS16 multiframing enabled. • Other—Line type that is other than those described by this parameter.
Line Code	Indicates the type of zero code suppression used on the line, which affects a number of its characteristics. Values include: • JBZS—Jammed Bit Zero Suppression. A technique in which the AT&T specification of at least one pulse every 8-bit period is literally implemented by forcing a pulse in bit 8 of each channel. Therefore, only seven bits per channel, or 1.344 Mbps, is available for data. • B8ZS—Bipolar with 8 Zeros Substitution. A specified pattern of normal bits and bipolar violations replace a sequence of eight zero bits. • ZBTSI—Zero Byte Time Slot Interchange. A technique applied to a DS1 frame to ensure pulse density requirements are met. ANSI clear channels use ZBTSI. • AMI—Alternate Mark Inversion. A technique in which no zero code suppression is present and the line encoding does not directly solve the problem. In this application, the higher layer must provide data which meets or exceeds the pulse density requirements. E1 links, with or without CRC, use this code or the HDB3 code. • HDB3—High Density Bipolar of order 3. A line code based on AMI. • Other—Line code that is other than those described by this parameter.
Send Code	Indicates what type of code is sent across the DS1 interface by the device. Values include: • Send No Code—Sending looped or normal data. • Send Line Code—Sending a request for a line loopback. • Send Payload Code—Sending a request for a payload loopback. • Send Reset Code—Sending a loopback termination request. • Send QRS—Sending a quasi-random signal (QRS) test pattern. • Send 511 Pattern—Sending a 511 bit fixed test pattern. • Send 3-in-24 Pattern—Sending a fixed test pattern of 3 bits set in 24. • Send Other Test Pattern—Sending a test pattern other than those described by this parameter.

Parameter	Value
Circuit Identifier	Contains the transmission vendor's circuit identifier, for the purpose of facilitating troubleshooting.
Loopback Config	Identifies the loopback configuration of the DS1 interface. Agents supporting read/write access should return badValue in response to a requested loopback state that the interface does not support. Values include: • No Loop—Not in the loopback state. A device that is not capable of performing a loopback on the interface always returns this value. • Payload Loop—The received signal at this interface is looped through the device. Typically the received signal is looped back for retransmission after it has passed through the device's framing function. • Line Loop—The received signal at this interface does not go through the device (minimum penetration) but is looped back out. • Other Loop—Loopbacks that are not defined by this parameter.
Signal Mode	Identifies the signal mode of the interface. Values include: • None—Indicates that no bits are reserved for signaling on this channel. • Robbed Bit—Indicates that T1 robbed bit signaling is in use. • Bit Oriented—Indicates that E1 channel associated signaling is in use. • Message Oriented—Indicates that common channel signaling is in use either on channel 16 of an E1 link or channel 24 of a T1.
Clock Source	Indicates the source of the transmit clock. Values include: • Loop Timing—Indicates that the recovered receive clock is used as the transmit clock. • Local Timing—Indicates that a local clock source is used. • Through Timing—Indicates that a recovered receive clock from another interface is used as the transmit clock.
Facilities Data Link	Describes the use of the facilities data link, and is the sum of the capabilities: • ANSI T1 403—Refers to the facilities data link (FDL) exchange recommended by ANSI. • AT&T 54016—Refers to ESF FDL exchanges. • FDL None—Indicates that the device does not use the FDL. • Other—Indicates use of a protocol other than those described by this parameter.

Line Status Information Pane

The Line Status Information pane contains:

Parameter	Value
Line Status	Indicates the line status of the interface. It contains loopback, failure, received alarm, and transmitted alarm information. Values include: • No Alarm—No alarm is present on the line. • Receive Far End LOF—Far end loss of frame (LOF). This notification is also known as a yellow alarm. • Transmit Far End LOF—Near end is sending LOF indication. • Receive AIS—Far end is sending alarm indication signal (AIS). • Transmit AIS—Near end is sending AIS. • Loss of Frame—Near end LOF (red alarm). • Loss of Signal—Near end loss of signal (LOS). • Loopback State—Near end is looped. • T16 AIS—E1 T16 alarm indication signal. • Receive Far End LOMF—Far end is sending T16 loss of multiframe (LOMF). • Transmit Far End LOMF—Near end is sending T16 LOMF alignment. • Receive Test Code—Near end is detecting a test code. • Other Failure—Any line status not defined by this parameter.
Loss of Frame Count ¹	Real-time count for loss of frame.
Loss of Signal Count ¹	Real-time count for loss of signal.
Remote Alarm Indication Count ¹	Real-time count for remote alarm indication.
Alarm Indication Signal Count ¹	Real-time count for alarm indication signal.

1. Not available for T1 or E1 controllers for ITP 12.2 releases.

Performance and Error Information Pane

The Performance and Error Information pane contains:

Parameter	Value
Time Elapsed within Interval	The number of minutes and seconds that have elapsed since the beginning of the current error-measurement period.
Line Code Violations	The number of line code violations (LCVs) encountered by the interface in the current 15-minute interval.
Path Coding Violations	The number of path coding violations encountered by the interface in one of the previous 96, individual 15-minute, intervals.

Parameter	Value
Slip Duration	The number of slip seconds encountered by the interface in the current 15-minute interval.
Severely Errored Framing Duration	The number of severely errored framing seconds encountered by the interface in the current 15-minute interval.
Line Error Duration	The number of line errored seconds encountered by the interface in the current 15-minute interval.
Degraded Duration	The number of degraded seconds encountered by the interface in the current 15-minute interval.
Errored Duration	The number of errored seconds encountered by the interface in the current 15-minute interval.
Bursty Error Duration	The number of bursty errored seconds encountered by the interface in the current 15-minute interval.
Severely Errored Duration	The number of severely errored seconds encountered by the interface in the current 15-minute interval.
Unavailable Duration	The number of unavailable seconds encountered by a DS1 interface in the current 15 minute interval.

Viewing RAN-O Performance Data



Note

The web interface provides historical (not real-time) charts depicting performance information over user-specified time ranges. You can use historical statistics for capacity planning and trend analysis. See [Displaying RAN-O Historical Statistics, page 11-33](#).

The MWTM client interface provides access to RAN-O real-time performance statistics that you can use to troubleshoot problems that occur in real time. The zoom and navigation features quickly enable isolating and focusing on a problem area.

You use real-time charts in the MWTM client to view performance information on shorthaul and backhaul interfaces. To view performance data for a shorthaul or backhaul interface, select the interface in the navigation tree of the DEFAULT view (or any custom view), then click the Backhaul or Shorthaul Performance tab in the right pane.



Note

If the CISCO-IP-RAN-BACKHAUL-MIB on the node is not compliant with the MWTM, the MWTM issues the message:

```
MIB not compliant for reports
```

Install a version of IOS software on the node that is compatible with the MWTM. For a list of compatible IOS software, from the MWTM:

- Web interface, choose **Administrative > IPRAN OS README**.
- Client interface, choose **View > Web > Administrative**; then click **IPRAN OS README**.

The Backhaul or Shorthaul Performance tab displays one or more charts depending on whether you selected a shorthaul or a backhaul interface. These charts depict send and receive rates of optimized IP traffic over time. The charts display the traffic from 0 to the maximum speed on the interface. You can set the client preferences to display this data in bits or bytes per second. The default polling interval is 15 seconds, but you can change the frequency in the Poller Settings dialog box, which you launch by clicking the Change Poller button.

The Backhaul or Shorthaul Performance tab also shows total send and receive errors when you select a backhaul interface.

This section provides information about:

- [Viewing Shorthaul Performance Data, page 8-108](#)
- [Viewing Backhaul Performance Data, page 8-111](#)

Viewing Shorthaul Performance Data

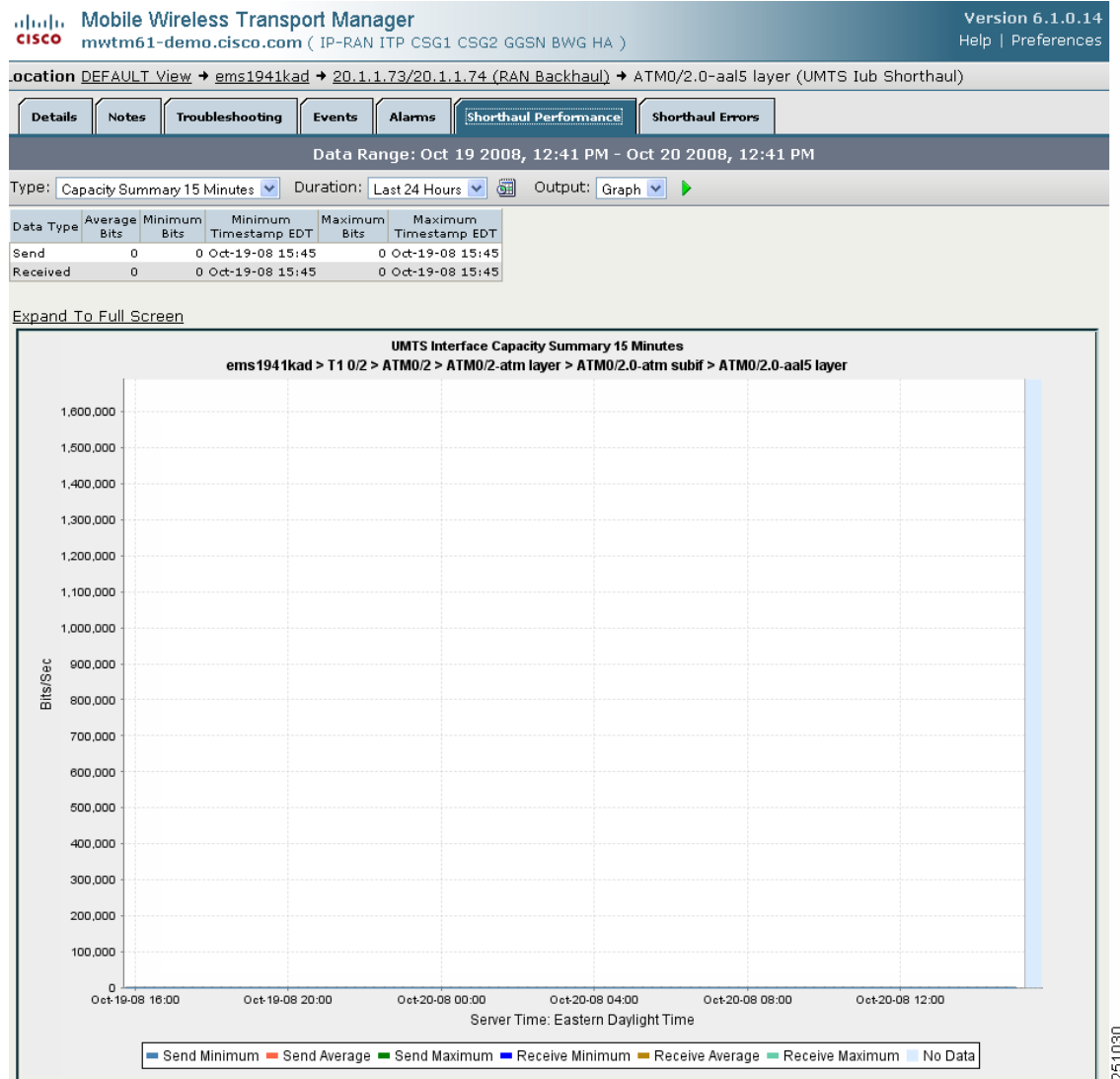


Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

The Shorthaul Performance tab displays a single chart that shows:

- The send rate plotted in one color and the receive rate plotted in a different color ([Figure 8-5](#)).
- A vertical band when the congestion mechanism is active (see the [Cisco MWR 1941-DC-A Mobile Wireless Edge Router Software Configuration Guide](#) for congestion management information).
- A different colored vertical band when no data exists.

Figure 8-5 Shorthaul Performance Tab

251030

Content Pane

The content (right) pane contains:

GUI Elements	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller , page 8-110.
Poll Interval	Label that shows the current poll interval in seconds.
Bits or Bytes/Sec	Y-axis label that displays traffic rate in bits or bytes per second. The default is bits per second. The Y axis automatically scales to the interface speed. To change the charts to show bytes per second, uncheck the Show Details in Bits instead of Bytes check box in the Preferences window (General Display Settings , page 5-4).

GUI Elements	Description
Time	X-axis label that displays a real-time scale and the server time zone.
Legend	Identifies the data series currently showing in the chart. • No Data—Data is not available. A vertical bar appears in the chart. • Congestion Active—Shows when the shorthaul is in a congested state. A vertical bar appears in the chart. Note You can configure the congestion mechanism for low-latency GSM and UMTS traffic. Other traffic (for example, SNMP or file transfer) can be discarded without entering the congestion mechanism. For detailed information about GSM and UMTS congestion management, see the Cisco MWR 1941-DC-A Mobile Wireless Edge Router Software Configuration Guide.

Change Poller

To change the poll interval, click the **Change Poller** button. The MWTM displays the Poller Settings dialog box.

The Poller Settings window displays these labels and buttons for the chosen shorthaul or backhaul interface:

Label/Button	Description
Poll Interval (secs)	The poll interval, in seconds, for the chosen node. To set a new poll interval, click in the Poll Interval (secs) text box and enter a new value. The default value is 15 seconds. Valid values are between 5 and 60.
Current Poll Interval	Value of the poll interval currently in use.
Number of Polls Received	Number of polls received by the chosen node.
Running Time	Time in hours, minutes, and seconds that the poller is running.
Change	Changes the poll interval from the current setting to the value you have entered in the Poll Interval (secs) text box.
Close	Closes the Poller Settings window.
Help	Displays online help for the current window.

Right-click Menu

A right-click context menu provides options to navigate to the backhauls that are associated with the chosen shorthaul interface. You can also modify how the chart appears. The right-click menu contains:

Menu options	Description
Goto > <i>backhaul</i>	Opens the Backhaul Performance tab for the backhaul interface associated with the chosen shorthaul interface.
Show/hide right-click menu	Provides options to show or hide one or more parts of a data series. See Right-click Menu, page 8-95 , for descriptions of the options.

Viewing Backhaul Performance Data

**Note**

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

The Backhaul Performance tab displays multiple charts in a split pane ([Figure 8-6](#)). The top pane displays send rate statistics, and the bottom pane displays receive rate statistics. You can maximize either pane to full screen size by using the split-pane control bar.

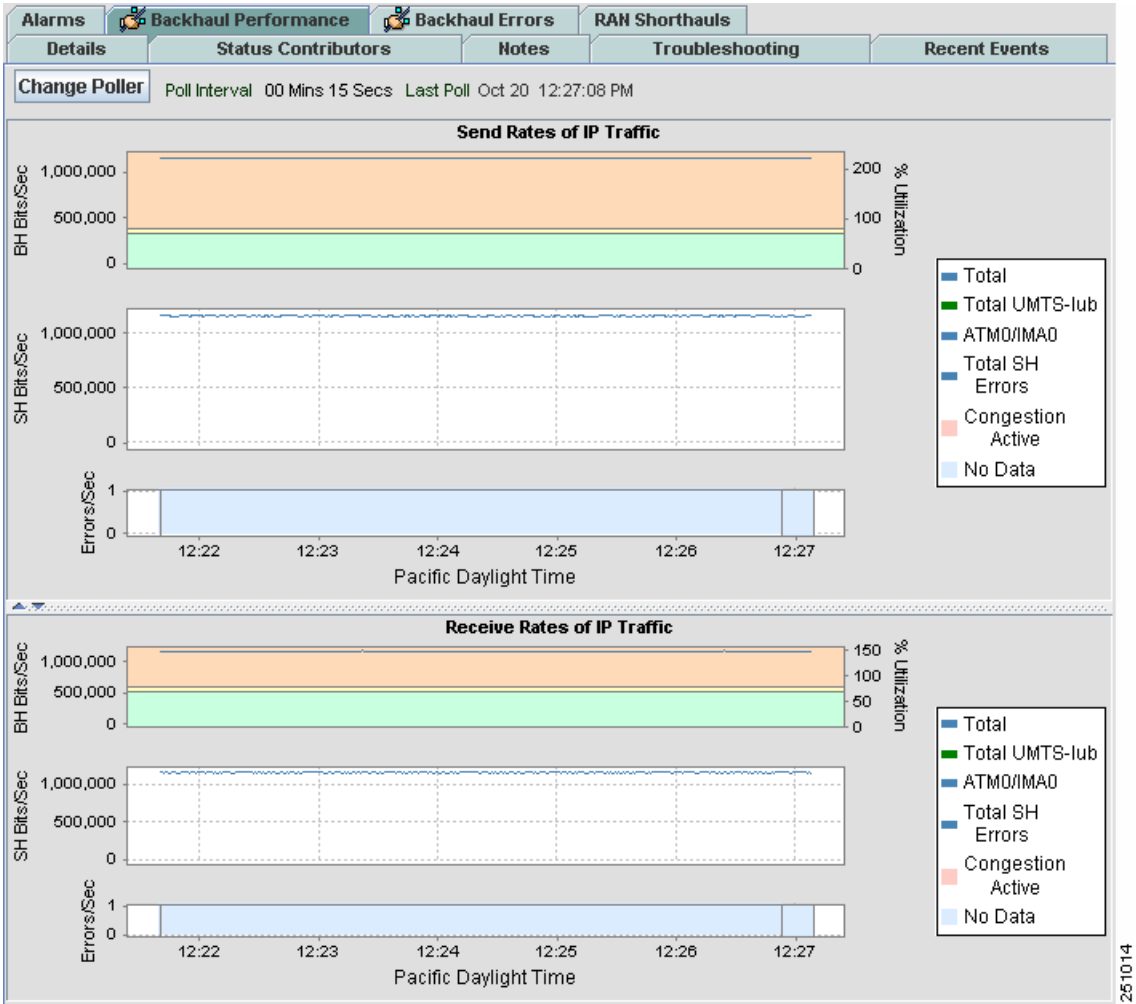
Each pane contains three charts that share the same time domain:

- **Top chart**—Displays total GSM traffic, total UMTS traffic, and total traffic (a summation of total GSM and total UMTS) in bits or bytes per second (left Y axis). The right Y axis displays the backhaul utilization as a percentage of the user bandwidth. You can change the scale of the Y axis by changing the User Bandwidth (see [Editing Properties for a RAN-O Backhaul, page 6-36](#)). The Y axis automatically scales to the User Bandwidth.

The top chart overlays the traffic display on top of threshold ranges (acceptable, warning, and overloaded) that are represented by color-coded, horizontal bands.

- **Middle chart**—Displays the traffic rates in bits or bytes per second for each shorthaul interface that is associated with the backhaul interface.
- **Bottom chart**—Displays total send-and-receive errors per second over time for all of the shorthaul interfaces included in the backhaul interface.

Figure 8-6 Backhaul Performance Tab



Content Pane

The content (right) pane contains:

GUI Elements	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Poll Interval	Label that shows the current poll interval in seconds.
SH or BH Bits or Bytes/Sec	Left Y-axis label that displays shorthaul (SH) or backhaul (BH) traffic rate in bits or bytes per second. The default is bits per second. This label appears for only the top and middle charts of both panes. The Y axis automatically scales to the User Bandwidth. To change the charts to show bytes per second, uncheck the Show Details in Bits instead of Bytes check box in the Preferences window (General Display Settings, page 5-4).

GUI Elements	Description
% Utilization	Y-axis label on the right side of the chart. The right-side axis displays the backhaul utilization as a percentage of the User Bandwidth. The chart background is color-coded to indicate these thresholds: • Overloaded—Top portion of chart background • Warning—Middle portion of chart background • Acceptable—Bottom portion of chart background For definitions of these thresholds, see Threshold Information (RAN-O Only), page 8-43. To change threshold settings, including the User Bandwidth, see Editing Properties for a RAN-O Backhaul, page 6-36. Note If the % Utilization exceeds 100%, see Why does my backhaul utilization graph show greater than 100% for transmit traffic?, page C-22.
Errors/Sec	Y-axis label that displays the total number of errors per second for send and receive traffic. This label appears only for the bottom chart of both panes. Note The same Errors/Sec chart appears in each pane.
Time	X-axis label that displays real-time scales for all the charts in the pane. The chart also shows the server time zone.
<i>Split-pane Control</i> 	Pane sizing feature that separates the top and bottom panes. To fully expand the: • Bottom pane, click the noninverted triangle on the control bar. • Top pane, click the inverted triangle on the control bar. To partially expand a pane, left-click the control bar and drag it up or down.
<i>Legend</i>	Color-coded legend to the right of the charts that describes the information that appears in all three charts of the pane.

Right-click Menu

A right-click context menu provides options to navigate to the shorthauls that are associated with the chosen backhaul interface. You can also modify how the chart appears.

The right-click menu contains:

Menu options	Description
Goto > <i>shorthaul</i>	Opens the Shorthaul Performance tab for the shorthaul interface associated with the chosen backhaul interface.
Display Series...	Opens the Display Series dialog box, which allows you to select data series to show or hide. See Display Series Dialog Box , page 8-113.
Reset Zoom, Grid, Shapes	See Right-click Menu , page 8-95, for descriptions of these options.

Display Series Dialog Box

The Display Series dialog box allows you to select data series to show or hide.

The Display Series dialog box contains:

Column or Button	Description
Display	Column of check boxes that allow you to display (by checking) or hide (by unchecking) the data series associated with the chosen backhaul. The MWTM displays no more than 12 series by default. You can change this setting for the MWTM Client Display or the MWTM Web Display: MWTM Client Display To change the maximum number of data series that the MWTM client interface displays by default, edit the MAX_CHART_SERIES parameter in the client-side <i>System.properties</i> file: - For the Windows client: <i>C:\Program Files\Cisco Systems\MWTM Client\properties\System.properties</i> - For Solaris or Linux client: <i>/opt/CSCOsgmClient/System.properties</i>  Caution Depending on the processing power and memory of your client system, setting the MAX_CHART_SERIES parameter too high can cause the client display to become unresponsive. If the client becomes unresponsive, set the MAX_CHART_SERIES to a lower value. Remember to restart the client to activate the new MAX_CHART_SERIES value. MWTM Web Display To change the maximum number of data series that the MWTM web interface displays by default, edit the MAX_CHART_SERIES parameter in the server-side <i>System.properties</i> file: <i>/opt/CSCOsgm/properties/System.properties</i>.  Caution Depending on the number of shorthauls that you display, setting the MAX_CHART_SERIES parameter too high can cause the web display to become unresponsive. If the web become unresponsive, set the MAX_CHART_SERIES to a lower value. Remember to restart the server to activate the new MAX_CHART_SERIES value.
Series Name	Name of the data series to display or hide.
RAN Backhaul	The RAN backhaul that is associated with the data series. This column appears only when the chosen backhaul is a virtual backhaul. For more information about virtual backhauls, see Creating Virtual RAN Backhauls, page 8-140.
Close	Closes the Display Series dialog box.
Help	Opens the help system for the Display Series dialog box.

Viewing RAN-O Error Data

**Note**

The web interface provides historical (not real-time) error information over user-specified time ranges. You can use historical statistics for capacity planning and trend analysis. See [Displaying RAN-O Historical Statistics, page 11-33](#).

The MWTM client interface provides access to RAN-O real-time error statistics that you can use to troubleshoot problems that occur in real time. The zoom and navigation features quickly enable isolating and focusing on a problem area.

You use real-time charts in the MWTM client to troubleshoot errors that occur on shorthaul and backhaul interfaces. To view error data for a shorthaul or backhaul interface, select it in the navigation tree of the DEFAULT view (or any custom view), and click the Shorthaul or Backhaul Errors tab in the right pane.

The Shorthaul or Backhaul Errors tab shows errors for the chosen interface.

**Note**

If the CISCO-IP-RAN-BACKHAUL-MIB on the node is not compliant with the MWTM, the MWTM issues the message:

MTB not compliant for reports

Install a version of IOS software on the node that is compatible with the MWTM. For a list of compatible IOS software, from the MWTM:

- Web interface, choose **Administrative > IPRAN OS README**.
- Client interface, choose **View > Web > Administrative**; then click **IPRAN OS README**.

Viewing Shorthaul Errors

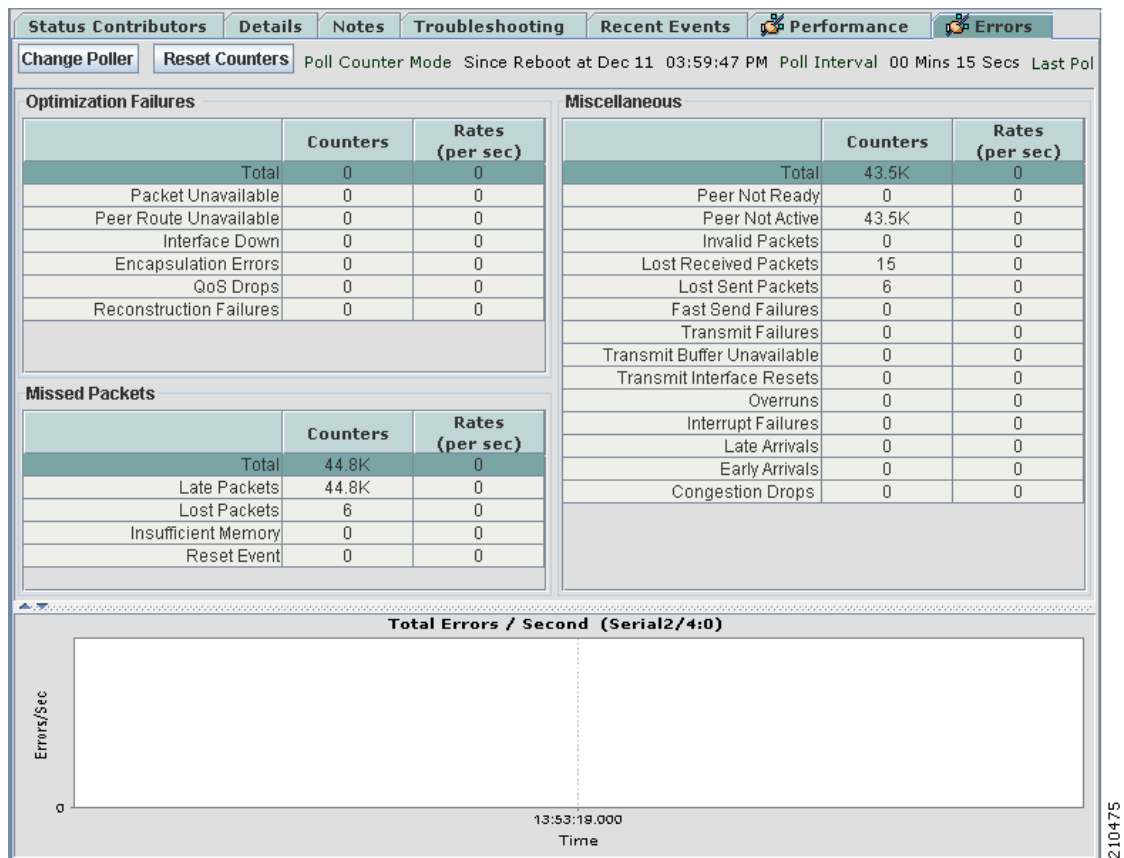
**Note**

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

When you select a GSM Abis shorthaul interface in the navigation tree in the DEFAULT view (or any custom view), the MWTM displays protocol, missed packet, and miscellaneous errors in the right pane ([Figure 8-7](#)). When you select a UMTS Iub shorthaul interface, the MWTM displays optimization and miscellaneous errors.

This window also includes a graph that displays the total number of errors per second. The graph has a right-click menu with options to similar to those of the right-click menu of the Performance window.

You can use the split pane control bar to resize or maximize the error tables or the error graph.

Figure 8-7 Example of Shorthaul Errors for GSM Abis Interface

Content Pane

The content (right) pane contains:

GUI Elements	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Reset Counters	Opens the Reset Counters dialog box to configure the method of polling. See Changing Real-Time Poller and Counter Settings, page 5-21 .
Poller Counter Mode	Label that displays the polling mode that you configure in the Reset Counters dialog box.
Poll Interval	Label that shows the current poll interval in seconds.
Optimization Failures	Pane that displays optimization failures for the chosen GSM Abis or UMTS Iub shorthaul interface. See Protocol Failures, page 8-117 .
Miscellaneous	Pane that displays miscellaneous errors on the chosen shorthaul interface. See Miscellaneous, page 8-118 .
	Note This pane appears for both GSM Abis and UMTS Iub shorthaul interfaces but with some differences in the types of errors shown.

GUI Elements	Description
Missed Packets	Pane that displays missed packet errors on the chosen GSM Abis shorthaul interface. See Missed Packets, page 8-119. Note This pane appears only for GSM Abis shorthaul interfaces.
Split-pane Control Bar 	Pane sizing feature that separates the top and bottom panes. To fully expand the: - Bottom pane, click the noninverted triangle on the control bar. - Top pane, click the inverted triangle on the control bar. To partially expand a pane, left-click the control bar and drag it up or down.
Total Errors / Second	Chart that displays the total number of errors per second on the shorthaul interface. See Total Errors per Second, page 8-120.

Protocol Failures

The Protocol Failures pane has a table that contains:

GUI Elements	Description
<i>Columns</i>	Table columns that list: <i>Type of error</i>—Type of protocol failure on the GSM Abis or UMTS Iub Counts—Number of errors of a particular type Rates (per sec)—Error rate for a particular type of error
Total	Total number of protocol failures encountered during the compression and decompression of the GSM-Abis or UMTS-Iub traffic.
Packet Unavailable	The number of times compression failed because a packet was unavailable.
Reconstruction Failures	The number of times information in a packet could not be decompressed.
Encapsulation Errors	The number of times compression failed because of encapsulation errors.
QoS Drops	The number of times compression failed because of quality of service errors or traffic load.
Peer Route Unavailable	The number of times compression failed because a route to the peer was not available.
Interface Down	The number of times compression failed because an interface was down.
Congestion Drops (GSM Abis only)	The number of dropped GSM packets or UMTS cells because of traffic congestion. Note You can configure the congestion mechanism for low-latency GSM and UMTS traffic. Other traffic (for example, SNMP or file transfer) can be discarded without entering the congestion mechanism. For detailed information about GSM and UMTS congestion management, see the Cisco MWR 1941-DC-A Mobile Wireless Edge Router Software Configuration Guide.

Miscellaneous

The Miscellaneous pane has a table that contains:



Note

The error types in the table apply to UMTS Iub and GSM Abis shorthaul interfaces unless otherwise noted.

GUI Elements	Description
<i>Columns</i>	Table columns that list: <i>Type of error</i>—Type of miscellaneous error on the GSM Abis or UMTS Iub shorthaul. Counts—Number of errors of a particular type. Rates (per sec)—Error rate for a particular type of error.
Total	Total number of miscellaneous failures encountered during the compression and decompression of the GSM-Abis or UMTS-Iub traffic.
Peer Not Ready	The count of packets dropped on the backhaul because the peer was not ready.
Peer Not Active (GSM Abis only)	The count of packets dropped on the backhaul because the peer was reachable but not in an active state.
Invalid Packets	The number of backhaul packets that were received and dropped because they contained invalid information.
Packet Allocation (UMTS Iub only)	The number of times a packet could not be allocated to send data on the UMTS Iub shorthaul interface.
Protocol Encapsulation Errors (UMTS Iub only)	The number of times compression failed because of encapsulation errors.
Local PVC Unavailable (UMTS Iub only)	The number of packets dropped because a local PVC was unavailable.
Remote PVC Unavailable (UMTS Iub only)	The number of packets dropped because a remote PVC was unavailable.
Backhaul Drops (UMTS Iub only)	The number of packets dropped on the backhaul.
Lost Received Packets (GSM Abis only)	The number of backhaul packets expected to be received but that never arrived.
Lost Sent Packets (GSM Abis only)	The number of backhaul packets sent but the peer never received.
Fast Send Failures (GSM Abis only)	The number of fast send failures on the shorthaul interface.
Transmit Failures (GSM Abis only)	The number of packet transmit failures on the shorthaul interface.

GUI Elements	Description
Interrupt Failures (GSM Abis only)	The number of packets lost due to interrupt failures.
Late Arrivals (GSM Abis only)	The number of GSM packets that arrived later than the allowed time.
Early Arrivals (GSM Abis only)	The number of GSM packets that arrived earlier than the allowed time.

Missed Packets

The Missed Packets pane appears only for GSM Abis shorthaul interfaces and has a table that contains:

GUI Elements	Description
<i>Columns</i>	Table columns that list: • <i>Type of error</i>—Type of missed packet error on the GSM Abis shorthaul interface. • Counts—Number of errors of a particular type. • Rates (per sec)—Error rate for a particular type of error.
Total	Total number of missed packet errors encountered during the compression and decompression of the GSM-Abis shorthaul interface.
Late Packets	The number of packets missed on the backhaul because they arrived past the allowed time frame
Lost Packets	The number of packets missed because they were lost on the backhaul
Overruns (GSM Abis only)	The number of packets missed due to the jitter buffer running out of available space.
Transmit Interface Resets (GSM Abis only)	The number of transmission interface resets.
Transmit Buffer Unavailable (GSM Abis only)	The number of times that the system is unable to allocate buffer for transmission.
Reset Event	The number of packets missed on the backhaul because of a reset event
Insufficient Memory	The number of packets missed on the backhaul for lack of available memory to allocate the packet

Total Errors per Second

The Total Errors per Second pane displays a chart that contains:

GUI Elements	Description
Total Errors/Second (shorthaul)	Chart title that lists the chosen shorthaul.
Errors/Sec	Y-axis label that displays errors per second for the chosen shorthaul.
Time	X-axis label that displays a real-time scale for the chosen shorthaul. The chart also displays the server time zone.

A right-click menu provides navigational and chart control options. See [Right-click Menu, page 8-110](#).

Viewing Backhaul Errors



Note

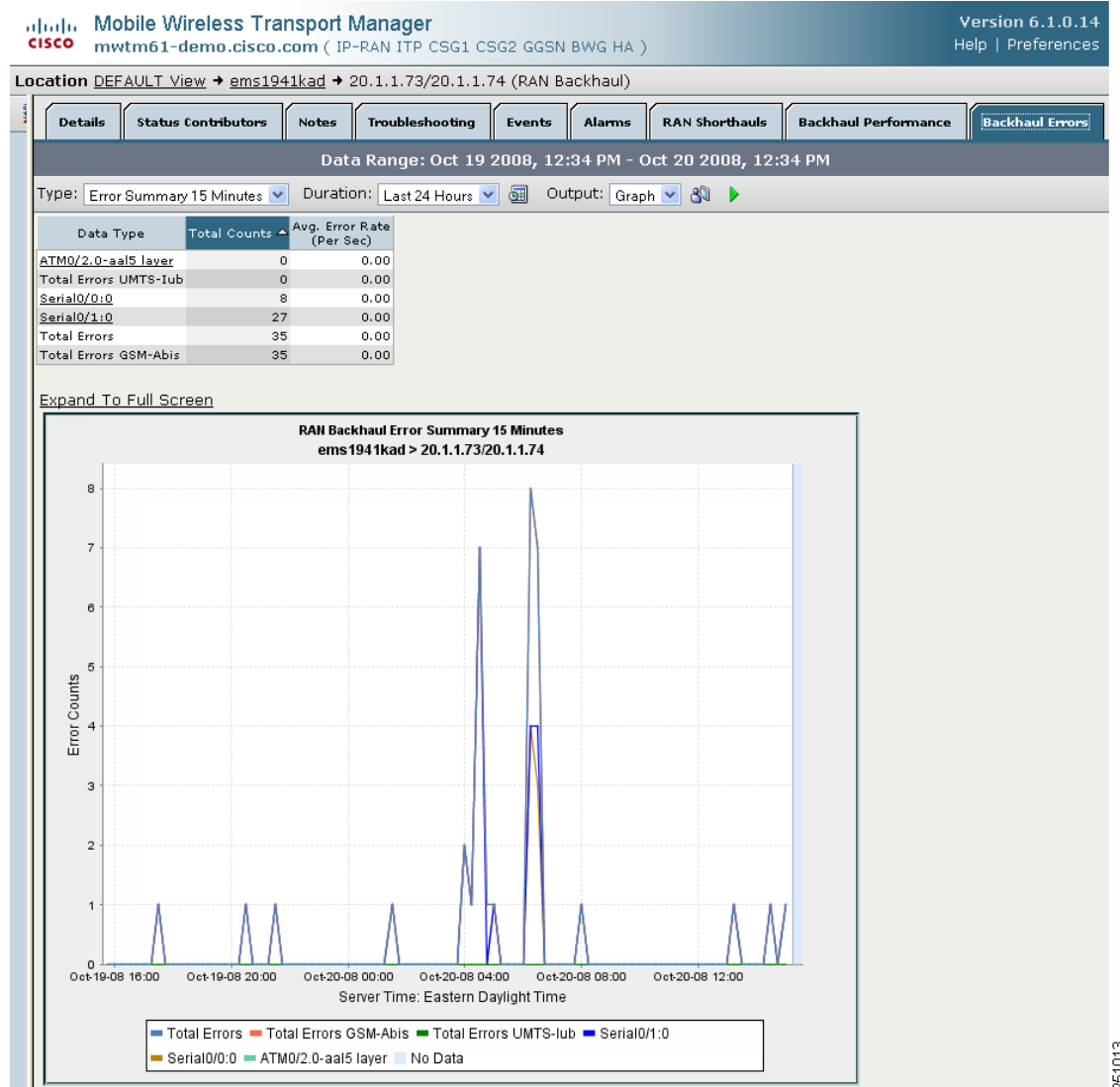
In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

When you select a backhaul interface in the navigation tree, the MWTM displays a chart in the right pane ([Figure 8-8](#)). The charts shows GSM and UMTS errors per second for each shorthaul interface included in the backhaul.

The content (right) pane contains:

GUI Elements	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Poll Interval	Label that shows the current poll interval in seconds.
Last Poll	Label that displays the date and time of the last poll.
GSM and UMTS Errors/Second	Chart title for GSM and UMTS errors.
Errors/Sec	Y-axis label that displays errors per second.
Time	X-axis label that displays a real-time scale and the server time zone.
<i>Legend</i>	Color-coded legend for the shorthaul interfaces included in the chosen backhaul.

A right-click menu provides navigational and chart control options. See [Right-click Menu, page 8-113](#).

Figure 8-8 Example of Backhaul Errors Chart

251013

Viewing PWE3 Statistics

You can view real-time Pseudowire Emulation Edge-to-Edge (PWE3) statistics for cell-site routers that have the PWE3 capability. To view real-time PWE3 statistics for one of these nodes, select the node in the navigation tree, then click the PWE3 Statistics tab. You can view real-time PWE3 statistics in the MWTM client and web interfaces (there are minor differences in layout and appearance).



Note

In the MWTM client, the real-time icon  appears in the tab. This icon indicates that polling will periodically occur while this window is open. To prevent unnecessary traffic on your network, close this window (for example, by clicking a different tab) when you no longer need to view the real-time data.

The PWE3 Statistics tab contains:

GUI Element	Description
Change Poller	Button that opens the Poller Settings dialog box. See Change Poller, page 8-110 .
Reset Counters	Button that opens the Reset Counters dialog box to configure the method of polling. See Changing Real-Time Poller and Counter Settings, page 5-21 .
Poller Counter Mode	Label that displays the polling mode that you configure in the Reset Counters dialog box.
Poll Interval	Label that shows the current poll interval in seconds.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
ID	Table column label that lists the ID of the virtual circuit.
Type	Type of service that carries the virtual circuit.
PSN Type	Type of packet-switched network (PSN) that carries the virtual circuit. For example, MPLS.
Name	Name of the virtual circuit.
Description	Description of the virtual circuit.
Peer Address	IP address of the peer node.
Create Time ¹	Time when the virtual circuit was created.
Up Time ¹	Length of time the virtual circuit has been operational.
Admin Status ¹	The administrative status of the virtual circuit.
Oper Status ¹	The operational status of the virtual circuit.
Inbound Oper Status ¹	The operational status of the virtual circuit in the inbound direction.
Outbound Oper Status ¹	The operational status of the virtual circuit in the outbound direction.
Time Elapsed ¹	Time in seconds since the beginning of the measurement period.
Valid Intervals ¹	Number of valid intervals for which data was collected.
Packets Received Rate	Number of packets that the virtual circuit received each second from the packet-switched network.
Packets Received Count ¹	Total number of packets that the virtual circuit received from the packet-switched network.
Bytes Received Rate	Number of bytes that the virtual circuit received each second from the packet-switched network.
Bytes Received Count ¹	Total number of bytes that the virtual circuit received from the packet-switched network.
Packets Sent Rate	Number of packets that the virtual circuit forwarded each second to the packet-switched network.
Packet Sent Count ¹	Total number of packets that the virtual circuit forwarded to the packet-switched network.

GUI Element	Description
Bytes Sent Rate	Number of bytes that the virtual circuit forwarded each second to the packet-switched network.
Bytes Sent Count ¹	Total number of bytes that the virtual circuit forwarded to the packet-switched network.

1. This column is hidden from view by default. To unhide the column, right-click in the column heading area and select the column label.

Viewing ITP Linkset Access Lists

The Linkset Access Lists section displays information about the access lists associated with the chosen linkset and its adjacent linkset.

To view the Linkset Access List section, in a view in the navigation tree, select an ITP linkset, then click on the Linkset Access Lists tab in the content area.



Note

This window polls your network periodically. To prevent unnecessary traffic on your network, close this window when you no longer need it.

This window is not available if the linkset is a Virtual linkset.

For each linkset, the Linkset Access Lists section displays these columns:

Column	Description
Poll Interval	Used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Linkset	Name of the linkset for which access lists appear.
In	Inbound access lists for the linkset. If the linkset has no inbound access lists, this field displays <code>None</code> .
Out	Outbound access lists for the linkset. If the linkset has no outbound access lists, this field displays <code>None</code> .
List #	Access list number configured on the node and applied to the linkset. ITP uses access list numbers 2700 through 2799.
Access List	List of commands in the access list.

Viewing Data Specific for ITP Signaling Points

These sections are specific only to ITP signaling points:

- [Viewing Route Detail, page 8-124](#)
- [Viewing GTT MAP Status, page 8-125](#)
- [Viewing GTT Statistics, page 8-126](#)

- [Viewing the MTP3 Event Log, page 8-129](#)
- [Viewing MLR Details, page 8-130](#)

Viewing Route Detail

The Route Detail table displays detailed information about routes associated with the chosen signaling point, including dynamic and shadow routes. The Route Detail table automatically eliminates duplicate data in successive rows.

To view the Route Detail section, in a view in the navigation tree, select an ITP signaling point, then click on the Route Detail tab in the content area.



Note

This window polls your network periodically. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

The Route Detail table displays these columns for the chosen signaling point:

Column	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description Polling node. After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Destination Point Code	Destination point code for packets on the chosen signaling point. The destination point code is the point code to which a given packet is routed.
Mask	Mask length for packets on the chosen signaling point. The mask length is the number of significant leading bits in the point code. The mask length is always 14 for ITU and 24 for ANSI.
Access	Status of the destination. Possible values are: • Accessible • Inaccessible • Restricted • Unknown
Congestion Level	Indicates the level of congestion on the route. A route is congested if it has too many packets waiting to be sent. This condition could be caused by the failure of an element in your network. Possible values for the Congestion Level field are <i>None</i> , indicating no congestion, and 1 to 7 , indicating levels of congestion from very light (1) to very heavy (7).
Number of Routes	Number of routes to the chosen destination route set (Destination Point Code plus Mask).
Cost	Cost of the route to the destination, relative to other routes. The valid costs range from 1 (lowest cost and highest priority) through 9 (highest cost and lowest priority).

Column	Description
Destination Linkset	Destination linkset associated with the destination point code. The destination linkset is also called the output linkset.
QoS	Quality of service (QoS) class of the route, as configured by the network administrator. Valid QoS classes range from 1 through 7 ; ALL indicates that the route accepts all QoS classes.
Management Status	Accessibility of the destination from the adjacent point code at the remote end of the signaling point. Possible values are: • Allowed—Traffic is allowed on the route without restriction. • Prohibited—Traffic is prohibited on the route. • Restricted—Traffic is restricted on the route. • Unknown—Accessibility cannot be determined.
Route Status	Status of the route. Possible values are: • Available • Restricted • Unavailable

Viewing GTT MAP Status

The GTT MAP Status table displays detailed information about all GTT MAPs associated with the chosen signaling point. The GTT MAP Detail table automatically eliminates duplicate data in successive rows.

To view the GTT MAP Status section, in a view in the navigation tree, select an ITP signaling point, then click on the GTT MAP Status tab in the content area.



Note

This window polls your network periodically. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

The GTT MAP Status table displays these columns for the chosen signaling point:

Column	Description
Reset Counters	Opens the MWTM Reset Counters dialog box, which you use to change MWTM poller and counter settings. For more information, see Changing Real-Time Poller and Counter Settings, page 5-21 .
Poll Counter Mode	Displays the current mode for poll counters, and the date and time that counters were last reset. Possible modes are: • Since Reboot—Counters display values aggregated since the last reboot of the ITP, or since ITP last reset the counters. • Since Last Poll—Counters display values aggregated since the last poll. • Since User Reset—Counters display values aggregated since the last time they were reset by the user.
Poll Interval	Poll interval used to collect data for the table.

Column	Description
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Point Code	Primary point code for the GTT MAP.
Point Code Status	Status of the primary point code. Possible values are: - Allowed Prohibited—Either the point code cannot be reached, or the point code is labeled Prohibited by the SCCP protocol.
Congestion Level	MTP3 congestion level for the primary point code. Possible values are: No congestion—Corresponds to None. The link is not congested. Congestion level 1—Corresponds to Low. The link is slightly congested. Congestion level 2—Corresponds to High. The link is congested. Congestion level 3—Corresponds to Very High. The link is very congested. Low, High, and Very High correspond roughly to equivalent ANSI, China standard, ITU, NTT, and TTC congestion levels.
Point Code Congested	Number of times a point code was congested at the GTT MAP.
Point Code Unavailable	Number of times a point code was unavailable at the GTT MAP.
SCCP Unavailable	Number of times an SCCP was unavailable at the GTT MAP.
MTP3 Failures	Number of times the MTP3 layer failed at the GTT MAP.
Number of Subsystems	Number of subsystems for the GTT MAP.
Subsystem Number	Primary subsystem number (SSN) for the GTT MAP.
Subsystem Status	Status of the primary SSN. Possible values are: - Allowed - Prohibited—Either the remote subsystem cannot be reached, or the SCCP protocol labels the subsystem Prohibited.
Subsystem Unavailable	Number of times a subsystem was unavailable at the GTT MAP.
Subsystem Congested	Number of times a subsystem was congested at the GTT MAP.

Viewing GTT Statistics

The GTT Statistics table displays detailed statistical information about all GTTs that are associated with the chosen signaling point. The GTT Statistics table automatically eliminates duplicate data in successive rows.

To view the GTT Statistics section, in a view in the navigation tree, select an ITP signaling point, then click on the GTT Statistics tab in the content area.

**Note**

This window polls your network periodically. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

The GTT Statistics table displays these columns for the chosen signaling point:

Column	Description
Reset Counters	Opens the MWTM Reset Counters dialog box, which you use to change MWTM poller and counter settings. For more information, see Changing Real-Time Poller and Counter Settings, page 5-21 .
Poll Counter Mode	Displays the current mode for poll counters, and the date and time that counters were last reset. Possible modes are: • Since Reboot—Counters display values aggregated since the last reboot of the ITP, or since ITP last reset the counters. • Since Last Poll—Counters display values aggregated since the last poll. • Since User Reset—Counters display values aggregated since the last time they were reset by the user.
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Uptime	Time the node is up, in days, hours, minutes, and seconds.
Selector Entries	Number of entries in the GTT Selector Table.
GTA Entries	Number of entries in the GTT GTA Table.
Application Group Entries	Number of entries in the GTT App Group Table.
Addr. Conversion Entries	Number of entries in the GTT Address Conversion Table.
Point Code List Entries	Number of entries in the GTT CPC List.
GTT Errors: Errors To MTP	Number of Error messages (ERRs) sent by GTT to the MTP.
GTT Errors: Errors From MTP	Number of Error messages (ERRs) received by GTT from the MTP.
GTT Errors: Translation Error	Number of times translation was requested for a combination of Translation Type, Numbering Plan, and Nature of Address for which no translation exists in the signaling point. Occurs when no selector is available for the combination of parameters provided in the MSU.
GTT Errors: Unequipped Subsystem Error	Number of times GTT could not perform a translation due to an unequipped subsystem.
GTT Errors: Q752 Unqualified Error	Number of times GTT could not perform a translation due to an error type not covered by the other, more specific error types.
GTT Errors: Invalid GTT Format	Number of times GTT detected an invalid global title format while performing translation.
GTT Errors: Hop Count Error	Number of times GTT detected a hop count violation in the MSU.

Column	Description
GTT Errors: MAP Not Found	Number of times a GTT to a point code or subsystem number was successful, but the point code or subsystem number was not found in the GTT MAP table.
GTT Errors: Counts	Number of GTT errors of the specified type since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data.
GTT Errors: Rate (per sec)	Number of errors that GTT detected per second.
GTT Messages: Total Messages	Number of messages that GTT handled from local and remote subsystems.
GTT Messages: Local Messages	Number of messages that GTT handled from local subsystems only.
GTT Messages: Total GTT Messages	Number of messages that GTT handled that require translation.
GTT Messages: UDT Messages Sent	Number of unitdata messages (UDTs) that GTT sent.
GTT Messages: UDT Messages Received	Number of unitdata messages (UDTs) that GTT received.
GTT Messages: UDTS Messages Attempted	Number of unitdata service messages (UDTSs) GTT attempted to send.
GTT Messages: UDTS Messages Sent	Number of unitdata service messages (UDTSs) that GTT sent.
GTT Messages: UDTS Messages Received	Number of unitdata service messages (UDTSs) that GTT received.
GTT Messages: XUDT Messages Sent	Number of extended unitdata messages (XUDTs) GTT sent.
GTT Messages: XUDT Messages Received	Number of extended unitdata messages (XUDTs) that GTT received.
GTT Messages: XUDTS Messages Attempted	Number of extended unitdata service messages (XUDTSs) GTT attempted to send.
GTT Messages: XUDTS Messages Sent	Number of extended unitdata service messages (XUDTSs) that GTT sent.
GTT Messages: XUDTS Messages Received	Number of extended unitdata service messages (XUDTSs) that GTT received.
GTT Messages: LUDT Messages Sent	Number of long unitdata messages (LUDTs) that GTT sent.
GTT Messages: LUDT Messages Received	Number of long unitdata messages (LUDTs) that GTT received.
GTT Messages: LUDTS Messages Sent	Number of long unitdata service messages (LUDTSs) that GTT sent.
GTT Messages: LUDTS Messages Received	Number of long unitdata service messages (LUDTSs) that GTT received.
GTT Messages: CR Sent To MTP	Number of Connection Request (CR) message that GTT sent to the MTP. This count includes ISDN-UP messages with embedded CRs.

Column	Description
GTT Messages: CR Received From MTP	Number of Connection Request (CR) message that GTT received from the MTP.
GTT Messages: CREF Sent To MTP	Number of Connection Refusal (CREF) messages that GTT sent to the MTP. This count includes ISDN-UP messages with embedded CRs.
GTT Messages: CREF Received From MTP	Number of Connection Refusal (CREF) messages that GTT received from the MTP.
GTT Messages: RSR Sent To MTP	Number of Reset Request (RSR) messages that GTT sent to the MTP.
GTT Messages: RSR Received From MTP	Number of Reset Request (RSR) messages that GTT received from the MTP.
GTT Messages: Counts	Number of GTT messages of the specified category since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data.
GTT Messages: Rate (per sec)	Number of errors messages handled by GTT, per second.

Viewing the MTP3 Event Log

The MTP3 Event Log table displays the most recent MTP3 events associated with the chosen signaling point.

To view the MTP3 Event Log section, in a view in the navigation tree, select an ITP signaling point, then click on the MTP3 Event Log tab in the content area.



Note

This window polls your network periodically. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

The MTP3 Event Log table displays these columns for the chosen signaling point:

Column	Description
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
Logged Events	Total number of MTP3 events that have been logged for this signaling point.
Dropped Events	Total number of MTP3 events that have been dropped for this signaling point.
Max Events	Maximum number of events that the event history can contain. When event history table is full, the oldest entries are deleted as new entries are added.
Allowed Events	ITP parameter that specifies the absolute maximum for the Max Events field. That is, for this node, the Max Events field can range from 0 to the value specified by the Allowed Events field.
Index	Event number that the ITP assigns.
Message	Message text for the event.

Viewing MLR Details

The MLR Details tab displays the MLR counters, trigger configuration, and trigger results associated with the chosen signaling point.

To view the MLR Details section, in a view in the navigation tree, select an ITP signaling point, then click on the MLR Details tab in the content area.



Note

This window polls your network periodically. To prevent unnecessary traffic on your network, close this window when you no longer need to refer to it.

The MLR Details tab displays these columns for the chosen signaling point:

Column	Description
Reset Counters	Opens the MWTM Reset Counters dialog box, which you use to change MWTM poller and counter settings. For more information, see Changing Real-Time Poller and Counter Settings, page 5-21 .
Poll Counter Mode	Displays the current mode for poll counters, and the date and time that counters were last reset. Possible modes are: • Since Reboot—Counters display values aggregated since the last reboot of the ITP, or since ITP last reset the counters. • Since Last Poll—Counters display values aggregated since the last poll. • Since User Reset—Counters display values aggregated since the last time the user reset them.
Poll Interval	Poll interval used to collect data for the table.
Last Poll	Time the last poll was run. This field initially displays the description <code>Polling node</code> . After the first polling cycle, the MWTM populates this field with the actual time of the last poll.
MLR Counters	Displays the MLR Counters table. For more information, see Viewing MLR Counters, page 8-130 .
MLR Trigger Config	Displays the MLR Trigger Configuration table. For more information, see Viewing MLR Trigger Config, page 8-132 .
MLR Trigger Results	Displays the MLR Trigger Results table. For more information, see Viewing MLR Trigger Results, page 8-136 .

Viewing MLR Counters

The MLR Counters table displays MLR counters associated with the chosen signaling point.

You can resize each column, or sort tables based on the information in one of the columns. By default, the MWTM displays all of the columns in the MLR Counters table.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The MLR Counters table displays these columns for the chosen signaling point:

Column	Description
Processed: Routed	Total number of packets routed by MLR, and the packet routing rate in packets per second.
Processed: MAP SMS-MO	Number of MSUs of type GSM-MAP SMS-MO processed by MLR, and the GSM-MAP SMS-MO MSU processing rate in packets per second.
Processed: MAP SMS-MT	Number of MSUs of type GSM-MAP SMS-MT processed by MLR, and the GSM-MAP SMS-MT MSU processing rate in packets per second.
Processed: MAP SRI-SM	Number of MSUs of type GSM-MAP SRI-SM processed by MLR, and the GSM-MAP SRI-SM MSU processing rate in packets per second.
Processed: MAP AlertSc	Number of MSUs of type GSM-MAP AlertSc processed by MLR, and the GSM-MAP AlertSc MSU processing rate in packets per second.
Processed: ANSI-41 SMD-PP	Number of MSUs of type ANSI-41 SMD-PP processed by MLR, and the ANSI-41 SMD-PP MSU processing rate in packets per second.
Processed: ANSI-41 SMS Requests	Number of MSUs of type ANSI-41 SMSRequest processed by MLR, and the ANSI-41 SMSRequest MSU processing rate in packets per second.
Processed: ANSI-41 SMS Notifys	Number of MSUs of type ANSI-41 SMSNotify processed by MLR, and the ANSI-41 SMSNotify MSU processing rate in packets per second.
Aborts: Total Aborted	Total number of MSUs aborted by MLR, and the MSU abort rate in packets per second.
Aborts: No Resources	Number of MSUs aborted by MLR because of a shortage of resources, and the No Resources MSU abort rate in packets per second.
Aborts: Results Blocked	Number of MSUs aborted by MLR with a result of block, and the Results Blocked MSU abort rate in packets per second.
Aborts: GTI Mismatches	Number of MSUs aborted by MLR because of mismatched GTIs, and the GTI Mismatches MSU abort rate in packets per second.
Aborts: Address Conversion Failures	Number of MSUs aborted by MLR because of a failed GTA address conversion, and the Address Conversion Failures MSU abort rate in packets per second.
Aborts: Destination Unavailables	Number of MSUs aborted by MLR because the destination was unavailable, and the Destination Unavailables MSU abort rate in packets per second.
Aborts: No Server Aborted	Number of MSUs aborted by MLR because no server was available, and the No Server Aborted MSU abort rate in packets per second.
Continues: Total Continued	Total number of MSUs returned to SCCP by MLR with a result of <code>continue</code> , and the MSU return rate in packets per second.
Continues: Failed Triggers	Number of MSUs returned to SCCP by MLR because of no trigger match, and the Failed Triggers MSU return rate in packets per second.
Continues: Result Continueds	Number of MSUs returned to SCCP by MLR with a result of <code>continue</code> , and the Result Continueds MSU return rate in packets per second.
Continues: Result GTTs	Number of MSUs returned to SCCP by MLR with a result of GTT, and the Result GTTs MSU return rate in packets per second.

Column	Description
Continues: Unsupported SCCP Msg Types	Number of MSUs returned to SCCP by MLR because of unsupported message types, and the Unsupported SCCP Msg Types MSU return rate in packets per second.
Continues: Unsupported Segmented SCCP Msgs	Number of MSUs returned to SCCP by MLR because of unsupported segments, and the Unsupported Segmented SCCP Msg MSU return rate in packets per second.
Continues: Unsupported Messages	Number of MSUs returned to SCCP by MLR because of parse failures, and the Unsupported Messages MSU return rate in packets per second.
Continues: Parse Errors	Number of MSUs returned to SCCP by MLR because of parse errors, and the Parse Errors MSU return rate in packets per second.
Continues: No Results	Number of MSUs returned to SCCP by MLR with no results, and the No Results MSU return rate in packets per second.
Continues: No Server Continueds	Number of MSUs returned to SCCP by MLR because no server was available, and the No Server Continueds MSU return rate in packets per second.

Viewing MLR Trigger Config

The MLR Trigger Config table displays the MLR trigger configuration associated with the chosen signaling point, divided into these subtables:

- [Triggers, page 8-132](#)
- [SubTriggers, page 8-133](#)
- [Ruleset, page 8-134](#)
- [Rules, page 8-134](#)
- [Addresses, page 8-135](#)
- [Results, page 8-135](#)

Triggers

The Triggers subtable displays MLR trigger information associated with the chosen signaling point.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Triggers subtable except Set Name, Start Date, End Date, and Status.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Triggers subtable displays these columns for the chosen signaling point:

Column	Description
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the trigger.
Index	Index number associated with the trigger.
SubTriggers	Number of subtriggers associated with the chosen trigger.

Column	Description
Start Date	Date and time on which this trigger should begin filtering traffic. If no Start Date is configured, this field displays N/A.
End Date	Date and time on which this trigger should stop filtering traffic. If no End Date is configured, this field displays N/A.
Status	Current status of the trigger. Possible values are: • Active—A corresponding GTT table entry for the trigger or, if this is an MTP3 trigger, an available route to the appropriate point code exists. • Inactive—No corresponding GTT table entry or available route to the appropriate point code for the trigger. The trigger will never match and a configuration error is likely.
Action	Action taken by the trigger.
Prematches	Preliminary count of trigger matches.
Prematch Rate	Number of Prematches per second for the trigger.
Matches	Number of trigger matches with result <code>Action Performed</code> .
Match Rate	Number of Matches per second for the trigger.
Parameters	Parameters that control the behavior of the trigger.

SubTriggers

The SubTriggers subtable displays MLR subtrigger information associated with the chosen signaling point and trigger.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the SubTriggers subtable.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The SubTriggers subtable displays these columns for the chosen signaling point:

Column	Description
Trigger (in subtable heading)	Set name of the parent trigger with which the chosen subtrigger is associated.
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the subtrigger.
Index	Index number associated with the subtrigger.
Action	Action taken by the subtrigger.
Matches	Number of subtrigger matches with result <code>Action Performed</code> .
Match Rate	Number of Matches per second for the subtrigger.
Parameters	Parameters that control the behavior of the subtrigger.

Ruleset

The Ruleset subtable displays MLR ruleset information associated with the chosen signaling point and trigger or subtrigger.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Ruleset subtable except Start Date and End Date.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Ruleset subtable displays these columns for the chosen signaling point:

Column	Description
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the ruleset.
Start Date	Starting date and time for this ruleset to become active.
End Date	Ending date and time for this ruleset to become active.
Segmented	Indicates whether this ruleset should process segmented messages.
Protocol	Default protocol for rules in this ruleset.
Search Type	Search type that this ruleset should perform.

Rules

The Rules subtable displays MLR rules information associated with the chosen signaling point and ruleset.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Rules subtable except Set Name.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Rules subtable displays these columns for the chosen signaling point:

Column	Description
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the rule.
Index	Index number associated with the rule.
Operation Type	Types of messages on which this rule matches.
Protocol	Protocol used for matching by this rule.
Matches	Number of rule matches with result <code>Action Performed</code> .
Match Rate	Number of Matches per second for the rule.
Rule Parameters	Parameters that control the behavior of the rule.
Result Parameters	Parameters that control the behavior of the result associated with this rule.

Addresses

The Addresses subtable displays MLR address information associated with the chosen signaling point and rule.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Addresses subtable except Set Name.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Addresses subtable displays these columns for the chosen signaling point:

Column	Description
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the address.
Address Type	Type of address. The MWTM 6.1 supports these types of addresses: bch—Binary-coded hexadecimal gsmDa—Groupe Special Mobile (GSM) 7-bit default alphabet
Address Digits	Address digits to be matched.
Exact Match	Indicates whether an exact match to the Address Digits is required.
Matches	Number of address matches with result <i>Action Performed</i> .
Match Rate	Number of Matches per second for the address.
Result Parameters	Parameters that control the behavior of the result associated with this address.

Results

The Results subtable displays MLR results information associated with the chosen signaling point and rule or address.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Results subtable except Index.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Results subtable displays these columns for the chosen signaling point:

Column	Description
Ruleset (in subtable heading)	Ruleset associated with the results.
No Server Available Action (in subtable heading)	Default behavior if no result is available. Possible actions are: Discard—Discard the packet without forwarding it. Resume—Return the unmodified packet to the higher level protocols for default routing.
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the results.

Column	Description
Index	Index number associated with the results.
Type	Type of result. Possible values are: PC—Point code ASName—Application server name
Result	Destination point code or name of the result.
Weight	Weight for this result in its set of results.
Count	Number of times this result is encountered.
Count Rate	Number of times per second this result is encountered.

Viewing MLR Trigger Results

The MLR Trigger Results table displays the MLR results associated with the chosen signaling point. You can use this subtable to determine which triggers, subtriggers, rules, and addresses are causing a particular result to execute.

The MLR Trigger Results table contains:

- [Results, page 8-136](#)
- [Addresses, page 8-137](#)
- [Rules, page 8-137](#)
- [Ruleset, page 8-138](#)
- [SubTriggers, page 8-138](#)
- [Triggers, page 8-139](#)

Results

The Results subtable displays all MLR results information associated with the chosen signaling point. You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Results subtable except Index.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Results subtable displays these columns for the chosen signaling point:

Column	Description
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the results.
Index	Index number associated with the results.
Type	Type of result. Possible values are: PC—Point code ASName—Application server name
Result	Destination point code or name of the result.
Weight	Weight for this result in its set of results.

Column	Description
Count	Number of times this result is encountered.
Count Rate	Number of times per second this result is encountered.

Addresses

The Addresses subtable displays MLR address information associated with the chosen result.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Addresses subtable except Set Name.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Addresses subtable displays these columns for the chosen signaling point:

Column	Description
ResultSet (in subtable heading)	Set of results associated with the addresses.
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the address.
Address Type	Type of address. The MWTM 6.1 supports these types of addresses: bch—Binary-coded hexadecimal gsmDa—Groupe Special Mobile (GSM) 7-bit default alphabet
Address Digits	Address digits to be matched.
Exact Match	Indicates whether an exact match to the Address Digits is required.
Matches	Number of address matches with result <code>Action Performed</code> .
Match Rate	Number of Matches per second for the address.
Result Parameters	Parameters that control the behavior of the result associated with this address.

Rules

The Rules subtable displays MLR rules information associated with the chosen result.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Rules subtable except Set Name.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Rules subtable displays these columns for the chosen signaling point:

Column	Description
ResultSet (in subtable heading)	Set of results associated with the rules.
Entries (in subtable heading)	Total number of entries in the subtable.

Column	Description
Set Name	Set name associated with the rule.
Index	Index number associated with the rule.
Operation Type	Types of messages on which this rule matches.
Protocol	Protocol used for matching by this rule.
Matches	Number of rule matches with result Action Performed.
Match Rate	Number of Matches per second for the rule.
Rule Parameters	Parameters that control the behavior of the rule.
Result Parameters	Parameters that control the behavior of the result associated with this rule.

Ruleset

The Ruleset subtable displays MLR ruleset information associated with the chosen result.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Ruleset subtable except Start Date and End Date.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Ruleset subtable displays these columns for the chosen signaling point:

Column	Description
Rule Number (in subtable heading)	Index number of the rule with which this ruleset is associated.
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the ruleset.
Start Date	Starting date and time for this ruleset to become active.
End Date	Ending date and time for this ruleset to become active.
Segmented	Indicates whether this ruleset should process segmented messages.
Protocol	Default protocol for rules in this ruleset.
Search Type	Search type that this ruleset should perform.

SubTriggers

The SubTriggers subtable displays MLR subtrigger information associated with the chosen result.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the SubTriggers subtable.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The SubTriggers subtable displays these columns for the chosen signaling point:

Column	Description
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the subtrigger.
Index	Index number associated with the subtrigger.
Action	Action taken by the subtrigger.
Matches	Number of subtrigger matches with result <code>Action Performed</code> .
Match Rate	Number of Matches per second for the subtrigger.
Parameters	Parameters that control the behavior of the subtrigger.

Triggers

The Triggers subtable displays MLR trigger information associated with the chosen result.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM displays all of the columns in the Triggers subtable except Set Name, Start Date, End Date, and Status.

For detailed information on working in tables, see [Navigating Table Columns, page 5-24](#).

The Triggers subtable displays these columns for the chosen signaling point:

Column	Description
Ruleset (in subtable heading)	Ruleset with which this trigger is associated.
Entries (in subtable heading)	Total number of entries in the subtable.
Set Name	Set name associated with the trigger.
Index	Index number associated with the trigger.
SubTriggers	Number of subtriggers associated with the chosen trigger.
Start Date	Date and time on which this trigger should begin filtering traffic. If no Start Date is configured, this field displays N/A.
End Date	Date and time on which this trigger should stop filtering traffic. If no End Date is configured, this field displays N/A.
Status	Current status of the trigger. Possible values are: Active—Either there is a corresponding GTT table entry for the trigger or, if this is an MTP3 trigger, there is an available route to the appropriate point code. Inactive—There is no corresponding GTT table entry or available route to the appropriate point code for the trigger. The trigger will never match and a configuration error is likely.
Action	Action that the trigger takes.

Column	Description
Prematches	Preliminary count of trigger matches.
Prematch Rate	Number of Prematches per second for the trigger.
Matches	Number of trigger matches with result <code>Action Performed</code> .
Match Rate	Number of Matches per second for the trigger.
Parameters	Parameters that control the behavior of the trigger.

Viewing RAN Shorthauls

To view RAN shorthauls that are associated with a RAN-O backhaul, select the backhaul object in the navigation tree in the left pane, and click the RAN Shorthauls tab in the right pane. The right pane displays a tabular list of RAN shorthauls that are associated with the chosen backhaul.

To view descriptions of the columns of the RAN shorthauls table, see [RAN Shorthauls Table](#), page 6-27.

Creating Virtual RAN Backhauls

You use the MWTM to create a virtual RAN backhaul by grouping real backhauls. A virtual backhaul is useful if you have configured several RAN backhauls for the same interface. To view the utilization for that interface, create a virtual RAN backhaul that contains all the real backhauls that you have configured for the interface.



Note

When creating virtual RAN backhauls, observe the following restrictions:

- You cannot add a real backhaul to more than one virtual backhaul.
- To add a real backhaul to a virtual backhaul, you must first enable report polling on the node that is associated with the real backhaul. If you add a real backhaul to a virtual backhaul, and then disable report polling on the associated node, historical reporting for the virtual backhaul will not work! To restore historical reporting for the virtual backhaul, you must enable report polling on the associated node or remove the real backhaul from the virtual backhaul. To enable report polling on a node, you must access the node by using its command line interface.

To create a virtual RAN backhaul, right-click a RAN backhaul, then choose **Create Virtual RAN Backhaul**. The MWTM displays the Virtual RAN Backhaul Editor.

The Virtual RAN Backhaul Editor contains:

Field or Button	Description
Name	Name of the virtual RAN backhaul.
Available Backhauls	Pane that contains the Available Backhauls table, which contains these columns: • Name—Name of the RAN backhaul • Node—Node to which the RAN backhaul belongs

Field or Button	Description
Included Backhauls	Pane that contains the Included Backhauls table, which contains these columns: Name—Name of the RAN backhaul Node—Node to which the RAN backhaul belongs
Add	Adds the chosen backhaul to the Included Backhauls table.
Remove	Removes the chosen backhaul from the Included Backhauls table.
Save	Saves the virtual RAN backhaul and closes the Virtual RAN Backhaul Editor.
Cancel	Cancels the current operation and closes the Virtual RAN Backhaul Editor.
Help	Opens the Help window for this feature.

To create a virtual RAN backhaul:

-
- Step 1** Enable report polling on the nodes associated with the backhauls that you plan to add to the virtual backhaul.
- Step 2** Right-click a backhaul in the RAN Backhauls table or in a view in the navigation tree.
- Step 3** Choose **Create Virtual RAN Backhaul** in the right-click menu.
The Virtual RAN Backhaul Editor appears.
- Step 4** In the Available Backhauls pane, choose a backhaul from the table.
- Step 5** Click **Add** to add the chosen backhaul to the Included Backhauls table.
- Step 6** Repeat [Step 5](#) for each additional backhaul you want to include in the virtual backhaul.
- Step 7** To remove a backhaul from the Included Backhauls table, choose a backhaul from the table and click **Remove**.
- Step 8** In the Name field at the top of the dialog box, enter a name for the virtual backhaul.
- Step 9** Click **Save** to create the virtual RAN backhaul and close the dialog box.
-



CHAPTER 9

Managing Alarms and Events

You can use the Cisco Mobile Wireless Transport Manager (MWTM) to view information about alarms and events, including their associated network objects and related information.

This chapter includes:

- [Basic Concepts and Terms, page 9-1](#)
- [Displaying Active Alarms and Event History, page 9-8](#)
- [Managing Filters for Alarms and Events, page 9-17](#)
- [Viewing Properties for Alarms and Events, page 9-27](#)
- [Attaching a Note to an Alarm or Event, page 9-29](#)
- [Viewing Archived Event Files on the Web, page 9-30](#)
- [Viewing the Event Metrics Report on the Web, page 9-30](#)
- [Changing the Way the MWTM Processes Events, page 9-35](#)
- [Forwarding Events as Traps to Other Hosts, page 9-48](#)
- [Setting Sounds for Events at an MWTM Client, page 9-49](#)

Basic Concepts and Terms

This section contains these topics:

- [Event Definition, page 9-2](#)
- [Alarm Definition, page 9-2](#)
- [Event Processing, page 9-3](#)
- [Database Archiving, page 9-4](#)
- [File-based Archiving, page 9-8](#)

Event Definition

An event is a singular occurrence in time. Events are derived from incoming traps and notifications, detected status changes, and user actions. Examples of events include:

- Port status change
- Node reset
- Node becoming reachable by the management station

The MWTM writes events to the MWTM database once, and they never change. By definition, an event is a historical instance in time, and the MWTM does not modify any information about the event. It is important to understand that an event, once it occurs, does not change its status even when the conditions that triggered the event are no longer present.

To view a list of recent events, click **Event History** in the navigation tree of the client or web interface. To view archived events, click **Archived** in the web interface toolbar.

Alarm Definition

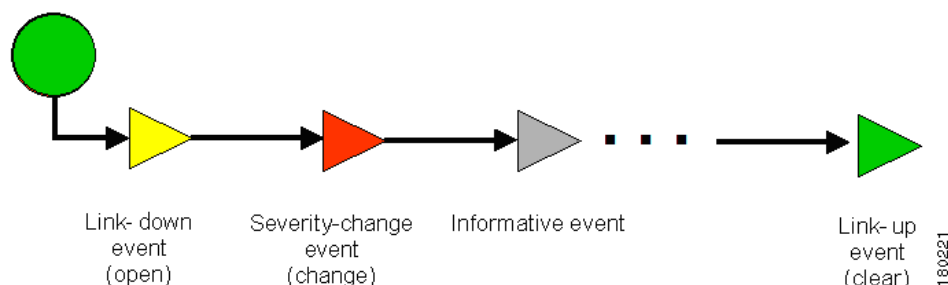
An alarm is a sequence of events, each representing a specific occurrence in the alarm lifecycle.

An alarm represents a series of correlated events that describe a fault occurring in the network or management system. An alarm describes the complete fault lifecycle, from the time that the alarm is raised (when the fault is first detected) until it is cleared and acknowledged. Examples of alarms include:

- Link down
- Device unreachable
- Card removed from slot

Figure 9-1 shows an example of a sequence of correlated events that describe the lifecycle of one alarm.

Figure 9-1 Example of Alarm



The MWTM constructs alarms from a sequence of correlated events. A complete event sequence for an alarm includes a minimum of two events:

- Alarm open (for example, a link-down event raises an alarm).
- Alarm clear (for example, a link-up event clears the alarm).

The lifecycle of an alarm can include any number of correlated events that are triggered by changes in severity, updates to services, and so on. When a new related event occurs, the MWTM correlates it to the alarm and updates the alarm severity and message text based on the new event. If you manually clear the alarm, the alarm severity changes to normal. You can still view the events that formed this alarm in the Event History table.

**Tip**

Remember that an alarm can change over time as new correlated events occur; but events, by definition, can never change. Events are historical instances in time.

To view all alarms, click **Active Alarms** in the navigation tree. By default, the navigation tree is sorted by alarm severity, with objects having the most severe alarms appearing at the top of the tree.

**Note**

While some events correlate to a single alarm, there are events that do not raise alarms at all.

Event Processing

This section contains these topics:

- [Event Queue Congestion, page 9-3](#)
- [Trap Rate Limits, page 9-3](#)

Event Queue Congestion

Event processing in the MWTM may occasionally experience congestion (for example, during discovery of very large networks). If the number of events exceeds the threshold of the event queue, the event congestion icon  appears in the lower left of the MWTM client and web windows. If the icon appears, the presentation of event information in the MWTM GUI will lag behind the actual state of network objects until the congestion clears. The event congestion icon will disappear from MWTM client and web windows when the congestion clears. No user action is necessary.

The event queue threshold is stored in the `EVENT_QUEUE_THRESHOLD_LIMIT` property in the `/opt/CSCOsrm/properties/Server.properties` file. The default setting is 1000 events.

Trap Rate Limits

If one or more nodes in the managed network begin to malfunction, these nodes can generate numerous trap notifications that trigger:

- An excessive number of events
- Excessive SNMP polling
- Increased database access

This condition is called a trap storm. In a large network, a trap storm can adversely affect the performance of the MWTM server. To minimize the effect of trap storms, the MWTM provides a server property to limit the trap rate of network nodes.

If a node in the network exceeds the trap rate threshold, the MWTM stops processing traps from that node. The MWTM raises an alarm (`TrapStatusAlarm`) to indicate that the node is generating excessive traps and that the MWTM has disabled trap processing for the node.

When you have corrected the problem with the faulty node and the trap rate is measured at a rate less than the `TRAP_RATE_LIMIT_COUNT` minus the `TRAP_RATE_ABATE_OFFSET`, the trap rate limit alarm will automatically clear and trap processing will automatically resume.

Though optional, you can clear the trap status alarm and re-enable trap processing for the node as described below:

-
- Step 1** In the navigation tree of the MWTM client, select the node.
- Step 2** Click the **Alarms** tab.
- Step 3** In the content pane, right-click the trap status alarm and choose **Clear** from the menu.
- Step 4** In the navigation tree, right-click the node and choose **Allow Trap Processing** from the menu.
-

The */opt/CSCOs/gm/properties/Server.properties* file provides these properties to limit the trap rate of managed nodes:

Server Property	Description
TRAP_RATE_ABATE_OFFSET	This is an offset value from the trap rate limit count. The abate threshold limit is calculated by subtracting this value from the TRAP_RATE_LIMIT_COUNT. The default value is 200 indicating if a node generates 2000-200 = 1800 or more traps it is still considered to be faulty and MWTM stops further trap processing for these nodes.
TRAP_RATE_LIMIT_COUNT	The threshold limit for a node. The default setting is 2,000. If a node generates 2,000 traps (or more) in the trap rate limit interval, the MWTM: • Raises a trap status alarm for the node • Disables trap processing for the node
TRAP_RATE_LIMIT_INTERVAL	The time interval for trap limitation. The default setting is 30 minutes. The MWTM scans its managed nodes every 30 minutes to determine if any nodes are exceeding the trap rate limit count.

Database Archiving

Database archiving describes the process by which the MWTM archives alarms and events in its database. The archival process for alarms and events follows this basic sequence:

1. An alarm or event occurs.
2. The alarm or event remains active for a configurable time period.
3. The MWTM archives the alarm or event in its database.
4. The alarm or event remains in archive for a configurable time period.
5. The MWTM deletes the alarm or event from the MWTM database.

The following sections go into greater detail about the archival process, including the differences between event and alarm archiving:

- [Event Archival Process, page 9-5](#)
- [Alarm Archival Process, page 9-6](#)

Event Archival Process

When you click Event History in the navigation tree of the MWTM client or MWTM web interface, the right pane displays a tabular list of recent events. The events that appear in this table remain active for seven days (this is the default setting). After seven days, the MWTM removes active events from the Event History table and archives them in the MWTM database. To view the archived events, go to the MWTM web interface, click Event History in the navigation tree, then click the Archived link in the tool bar.

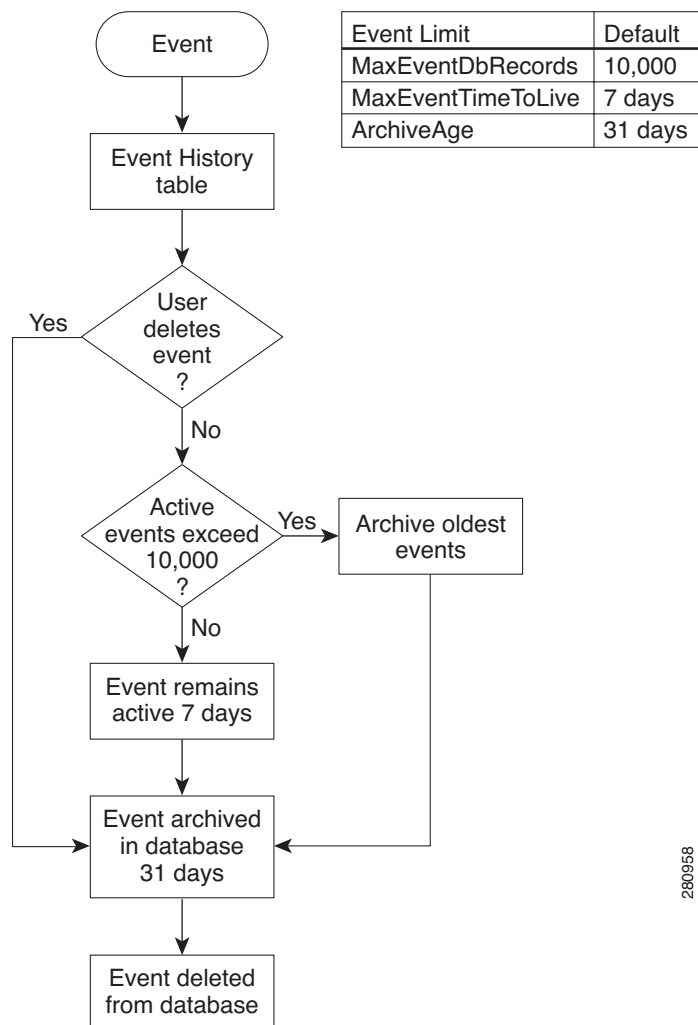
If a user manually deletes an event from the Event History table, the MWTM removes the event from the table and archives it in the MWTM database.

Also, if the number of active events exceeds 10,000 (this is the default setting), the MWTM archives the oldest events regardless of how long they have been active. This mechanism ensures optimal performance of the MWTM server and its clients.

The MWTM archives events in the MWTM database for 31 days (this is the default setting). After 31 days, the MWTM deletes the archived events from the MWTM database.

To change the default settings for archiving events, change the appropriate event limit. See [Changing Event Limits, page 9-37](#).

[Figure 9-2](#) illustrates the archival process for events and lists the event limits associated with the event archival process.

Figure 9-2 Event Archival Process

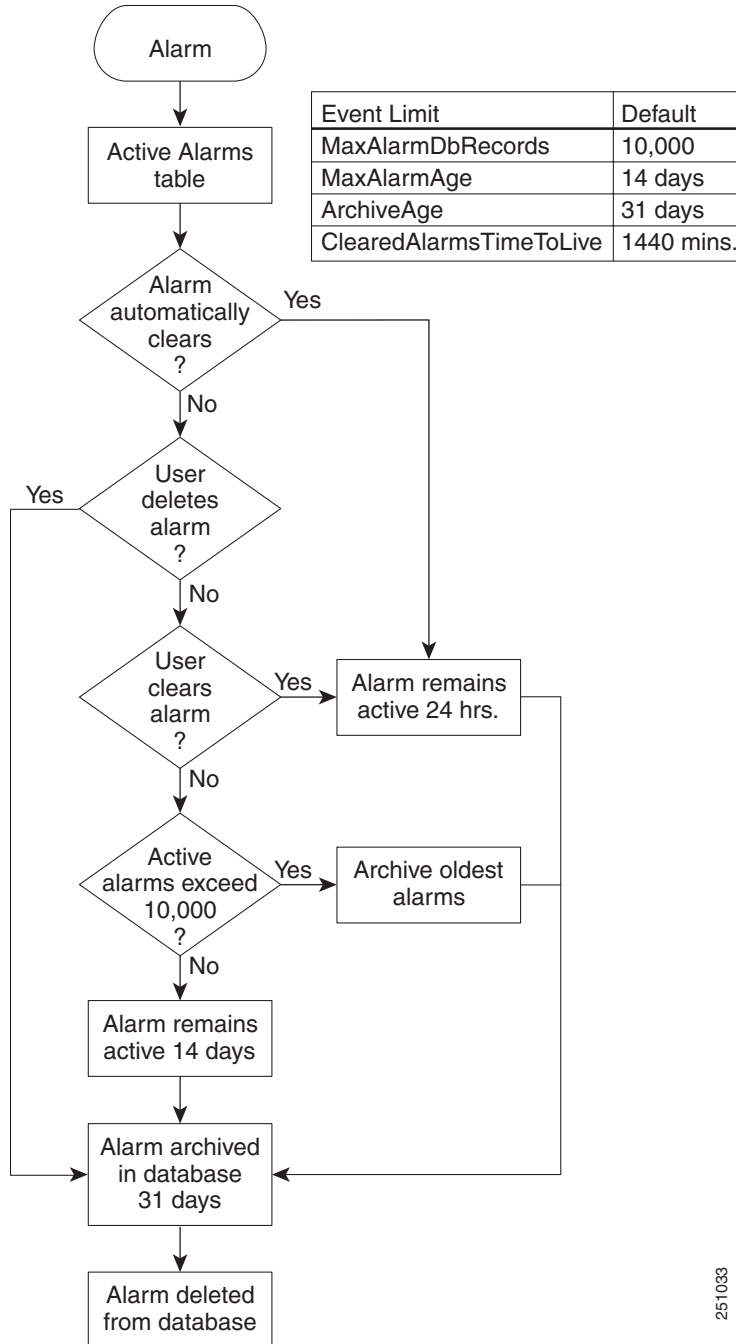
Alarm Archival Process

The archival process for alarms is very similar to the process for events. When you click Active Alarms in the navigation tree of the MWTM client or MWTM web interface, the right pane displays a tabular list of active alarms. The alarms that appear in this table remain active for 14 days (the default setting). After 14 days, the MWTM removes alarms from the Active Alarms table and archives them in the MWTM database. To view the archived alarms, go to the MWTM web interface, click Active Alarms in the navigation tree, then click the Archived link in the tool bar.

If the alarm automatically clears or if you manually delete the alarm from the Active Alarms table, the MWTM removes the alarm from the table and archives it in the MWTM database.

Likewise, if the alarm automatically clears or you manually clear an alarm from the Active Alarms table, the MWTM retains the alarm in the table for 1440 minutes, which is 24 hours (the default setting). After 24 hours, the MWTM removes the cleared alarm from the table and archives it in the MWTM database.

Figure 9-3 illustrates the archival process for alarms and lists the event limits associated with the alarm archival process.

Figure 9-3 Alarm Archival Process

Also, if the number of active alarms exceeds 10,000 (this is the default setting), the MWTM archives the oldest alarms regardless of how long they have been active. This mechanism ensures optimal performance of the MWTM server and its clients.

The MWTM archives alarms in the MWTM database for 31 days (this is the default setting). After 31 days, the MWTM deletes the archived alarms from the MWTM database.

To change the default settings for archiving alarms, change the appropriate event limit. See [Changing Event Limits](#), page 9-37.

File-based Archiving

The MWTM exports events and alarms from its database archives once a day and consolidates them into a CSV-based file. File-based archiving allows administrators to access archived events and alarms in a file format. For example, an administrator may want to process the contents of a file archive by using third-party scripting tools.

To view file-based archives, choose **FileArchive > Events** from the MWTM web interface. The MWTM displays file archives in the right pane. These examples illustrate the file-naming convention:

```
Status+Trap.WedJun04.log.csv.zip
Status+Trap.TueJun03.log.csv.zip
Status+Trap.MonJun02.log.csv.zip
```

The MWTM stores file archives in this directory:

```
/opt/CSCOsgm/logs/netstatus
```

If you want to change the default directory, use the `mwtm msglogdir` command.

The MWTM retains file archives for 31 days. (This default setting is the same value that is used for database archiving.) After 31 days, the MWTM deletes the files. If you want to change the default setting, use the `mwtm msglogage` command.

Another approach would be to configure the aging parameters of the file and database archives with different values. For example, you could use the default setting of 31 days to retain database archives but configure the file archive retention to 90 days (assuming your server has sufficient disk space). This file-based approach for long-term archiving is more efficient than retaining archives in the database beyond the 31-day default setting.

If required, you could retrieve file archives before the MWTM deletes them by using a backup system or a network file system that performs automatic file backups.

Displaying Active Alarms and Event History

You use the MWTM to view a network summary of active alarms and historical events. The contents of the Active Alarms window and the Event History window are very similar in appearance (the Active Alarms table shows fewer entries than the Event History table because multiple events are associated with a single alarm.)

Here are a few helpful facts about alarms and events:

- The MWTM displays the number of alarms or events in the message area (lower left area of the GUI).
- Not all events raise alarms.
- Alarms can be cleared and removed from the MWTM, while events cannot.

To see a summary of all active alarms, in the MWTM client or web interface, click **Active Alarms** in the navigation tree. The MWTM shows the Active Alarms window in the right pane (see [Figure 9-4](#)).

Figure 9-4 Active Alarms Window

Active Alarms

Last Updated 10/9/2008 11:51 AM

Page 1 of 22 (2193 entries)

Archived

Status Refresh Interval: 180 seconds

Page Size: 100

Severity: Critical

Change Severity

0 events selected

Clear Select

☐	Ack	Name	Severity	Count	Change Time	Message
☐		UserDbStateChanged	Minor	1	03:46:32 AM 10/9/08	emssami06.disco.com -- The CSG user database server 1.2.3.8:63101 is reset.
☐		UserDbStateChanged	Minor	1	03:45:55 AM 10/9/08	emssami14-1.disco.com -- The CSG user database server 5.5.5.5:2048 is reset.
☐		UserDbStateChanged	Minor	1	03:45:55 AM 10/9/08	emssami05.disco.com -- The CSG user database server 5.5.5.5:2048 is reset.
☐		SupplyStateChange	Major	1	03:11:21 AM 10/9/08	ems7604h.disco.com - Reported Supply state 'not functioning' on Power Supply 1, PWR-2700-AC/4.
☐		SupplyStateChange	Critical	1	03:10:14 AM 10/9/08	ems2941a.disco.com - Reported Supply state 'shutdown' on Brick Supply.
☐		SupplyStateChange	Critical	1	03:10:14 AM 10/9/08	ems2941a.disco.com - Reported Supply state 'shutdown' on Feed Supply.
☐		SupplyStateChange	Critical	1	03:10:14 AM 10/9/08	ems2941a.disco.com - Reported Supply state 'shutdown' on RPS Supply.
☐		SupplyStateChange	Major	1	03:10:09 AM 10/9/08	ems7604j.disco.com - Reported Supply state 'not functioning' on Power Supply 1, PWR-2700-AC/4.
☐		SupplyStateChange	Major	1	03:05:57 AM 10/9/08	sgm-76-92c-2.disco.com - Reported Supply state 'not functioning' on Power Supply 2, PWR-2700-AC.
☐		SupplyStateChange	Major	1	03:05:29 AM 10/9/08	sgm-76-94k.disco.com - Reported Supply state 'not functioning' on Power Supply 1, PWR-2700-AC/4.
☐		SgmpAssociationState	Major	1	03:07:40 AM 10/9/08	SGMP sgm-26-92b-2.disco.com/sg7390i added in state Inactive/SGMP Inactive.

The Active Alarms window provides basic information about all active alarms in your network, that are not excluded from your current view. The MWTM updates the information in the window at least once every minute. For more information about the Active Alarms window, see:

- [Toolbar Buttons, page 9-14](#)
- [Right-click Menus, page 9-16](#)

To see a summary of all the recent events, in the MWTM client or web interface, click **Event History** in the navigation tree. The MWTM shows the Event History window in the right pane (see [Figure 9-5](#)).

Figure 9-5 Event History Window

Recent Events

Last Updated 10/9/2008 11:30 AM

Page 1 of 101 (10014 entries)

 Archived

 **Status Refresh Interval:** 180 seconds

Page Size:



0 events selected [Clear Selection](#)

☐	Ack	Category	Severity	Create Time	Message
☐		Status	 Normal	12:59:54 PM 10/8/08	APN andywashere on GGSN emssami08-1.disco.com -- The APN is in service.
☐		Status	 Normal	12:59:53 PM 10/8/08	APN andywashere on GGSN emssami08-1.disco.com added in state Active/None.
☐		Status	 Informational	04:01:27 AM 10/8/08	APN apn_11 changed state from Active to Warning/SNMP Timeout.
☐		Status	 Normal	04:14:30 AM 10/8/08	APN apn_11 changed state from Warning to Active/None.
☐		Status	 Informational	04:01:27 AM 10/8/08	APN apn_11 on GGSN emssami12-1.disco.com changed state from Active to Unknown/SNMP Timeout.
☐		Status	 Normal	04:14:30 AM 10/8/08	APN apn_11 on GGSN emssami12-1.disco.com changed state from Unknown to Active/None.
☐		Status	 Informational	04:01:27 AM 10/8/08	APN apn_name changed state from Active to Warning/SNMP Timeout.
☐		Status	 Normal	04:14:30 AM 10/8/08	APN apn_name changed state from Warning to Active/None.
☐		Status	 Informational	04:01:27 AM 10/8/08	APN apn_name on GGSN emssami12-1.disco.com changed state from Active to Unknown/SNMP Timeout.
☐		Status	 Normal	04:14:30 AM 10/8/08	APN apn_name on GGSN emssami12-1.disco.com changed state from Unknown to Active/None.
☐		Status	 Informational	04:01:27 AM 10/8/08	APN dsfdffffdddddde changed state from Active to Warning/SNMP Timeout.

The Event History window shows information about the recent events that the MWTM event logger and event processor deliver for all objects in the current network view. The MWTM archives recent events after seven days (the default setting). For more information about the archival process, see [Managing Filters for Alarms and Events, page 9-17](#).

For more information about the Event History window, see:

- [Toolbar Buttons, page 9-14](#)
- [Right-click Menus, page 9-16](#)

**Note**

You can view multiple Event History windows at the same time, with different event filtering in each window or dialog box.

If you select a specific object in the navigation tree and click the Alarms tab or Recent Events tab, the MWTM shows information about the alarms or events for that object only.

You can resize each column (except when using the web interface), or sort the table based on the information in one of the columns.

**Note**

For more information about resizing, sorting, displaying, or hiding columns, see [Navigating Table Columns, page 5-24](#).

To see detailed information about an alarm or event, in the:

- MWTM client interface, right-click the event in a window, then select **Alarm and Event Properties** in the right-click menu.
- Web interface, select the alarm or event by checking its check box, then click the **Alarm and Event Properties** icon  in the toolbar.

**Note**

When using the web interface to select an alarm or event in the table, you check the check box for the row. You can select multiple rows. To clear the selection, click Clear Selection in the toolbar. In the client interface, use the Shift key to select multiple rows. To clear the selection, left-click anywhere in the table.

The table columns of the Active Alarms, Alarms tab, Event History, and Recent Events tabs include:

Column	Description
Internal ID	Internal ID of the alarm or event. The internal ID is a unique ID that the MWTM assigns for its own internal use. This ID can also be useful when the Cisco Technical Assistance Center (TAC) is debugging problems. This column is hidden by default.
Ack	Indicates whether the alarm or event has been acknowledged. To: • Acknowledge an unacknowledged alarm or event, use the Acknowledge toolbar button. • Make a previously acknowledged event unacknowledged, use the Unacknowledge toolbar button.
Name	Name of the alarm or event.

Column	Description
Element Name	Network element name associated with the event. This column is hidden by default.
Category	Type of the event. Default values include: • Create—Creation event, such as the creation of a seed file. • Delete—Deletion event, such as the deletion of an object or file. • Discover—Discovery event, such as Discovery beginning. • Edit—Edit event. A user has edited an object. • Ignore—Ignore event. A user has Ignored a link or linkset. • LaunchTerminal—An event related to the MWTM telnet or ssh terminal service. • Login—Login event. A user has logged in to the MWTM. • LoginDisable—LoginDisable event. The MWTM has disabled a user's User-Based Access authentication as a result of too many failed attempts to log in to the MWTM. • LoginFail—LoginFail event. An attempt by a user to log in to the MWTM has failed. • Logout—Logout event. A user has logged out of the MWTM. • OverWrite—OverWrite event. An existing file, such as a seed file or route file, has been overwritten. • Poll—Poll event, such as an SNMP poll. • Purge—Purge event. A user has requested Discovery with Delete Existing Data selected, and the MWTM has deleted the existing the MWTM database. • Provision—An event related to the MWTM device provisioning subsystem. • Status—Status change message generated. • Trap—SNMP trap message generated. You can customize this field (see Changing Event Categories, page 9-41). This column is hidden by default in the Active Alarms window and the Alarms tab.

Column	Description
Severity	Severity of the alarm or event. Possible severities are:  Critical  Major  Minor  Warning  Normal  Indeterminate  Informational You can customize this field (see Right-Click Menu for a Specific Alarm or Event, page 9-17). To change the severity of an alarm, in the: - MWTM client interface, right-click the alarm and choose Change Severity > <i>new severity</i> from the menu. - Web interface, select the event by checking its check box, choose a new severity from the Severity drop-down menu, then click the Change Severity button. Note You cannot change the severity of an event.
Original Severity	Original severity of the event. This column is hidden by default.
Count	Number of times this alarm occurred. This column is hidden by default in the Event History window and the Recent Events tab.
Note	Indicates whether a note is associated with the event. This column is hidden by default.
Create Time	Time this event was received. This column is hidden by default in the Active Alarms window and the Alarms tab.
Change Time	Time this event was last updated. This column is hidden by default in the Event History window and the Recent Events tab.
Ack By	If you have not implemented the MWTM User-Based Access, name of the node that last acknowledged the event. If you have implemented the MWTM User-Based Access, name of the user who last acknowledged the event. If no one has acknowledged the event, this field is blank. This column is hidden by default.
Node	Name of the node associated with the alarm or event. If no node is associated with the alarm or event, None appears. This column is hidden by default.
Card (RAN-O only)	Card associated with this alarm or event. This column is hidden by default.

Column	Description
SP (ITP only)	Name of the signaling point associated with the alarm or event. If no signaling point is associated with the alarm or event, None appears. This column is hidden by default.
Linkset (ITP only)	Name of the linkset associated with the alarm or event. If no linkset is associated with the alarm or event, None appears. This column is hidden by default.
Link (ITP only)	Name of the link associated with the alarm or event. If no link is associated with the alarm or event, None appears. This column is hidden by default.
SGMP (ITP only)	Name of the signaling gateway-mated pair associated with the alarm or event. If no signaling gateway-mated pair is associated with the alarm or event, None appears. This column is hidden by default.
ASP (ITP only)	Name of the application server process associated with the alarm or event. If no application server process is associated with the alarm or event, None appears. This column is hidden by default.
AS (ITP only)	Name of the application server associated with the alarm or event. If no application server is associated with the alarm or event, None appears. This column is hidden by default.
ASPA (ITP only)	Name of the application server process association associated with the alarm or event. If no application server process association is associated with the alarm or event, None appears. This column is hidden by default.
Interface	Interface associated with this alarm or event. This column is hidden by default.
RAN Backhaul (RAN-O only)	RAN backhaul associated with this alarm or event. This column is hidden by default.
Message	The message associated with the alarm or event.

Toolbar Buttons

The Active Alarms and Event History windows in the client and the web interfaces provide these toolbar buttons:

Button	Description
 Set Filter	Opens the Alarm and Event Filter dialog box.
 Apply Filter or  Remove Filter	Activates and deactivates the event filter specified in the Event Filter dialog box. If: - The filter is activated, the MWTM shows only those alarms or events that pass the filter. - The filter is deactivated, the MWTM shows all alarms or events. - You activate a filter in an object's Recent Events table in the MWTM main window, the filter is activated in all Recent Events tables in the MWTM main window for all other objects. The filter is not activated in Recent Events tables in Show In New Window windows or Real-Time Data and Charts windows.
 Show only Archived Events or Show only Archived Alarms (Client interface only)	In the Active Alarms page, the Show only Archived Alarms button takes you to the Archived Alarms page in the web. In the Event History page, the Show only Archived Events button takes you to the Archived Events page in the web.
Archived (web interface only)	This option appears in the tool bar when you are viewing the Event History table or the Active Alarms table. Click the Archived button to display a table of archived events or alarms. Click the Archived button again to switch back and forth.
 Refresh (web interface only)	Forces a refresh of the current web page. Click this icon to refresh the current page.



Caution

In the *Server.properties* file, you can limit the number of rows in the archived events table with the MAX_ARCHIVED_EVENT_DB_ROWS property. The default value is 200,000. Increasing this value can have severe impact on server performance and can cause the server to run out of memory.

Button	Description
 Pause or  Resume	Pauses or resumes the table. While the table is paused, the MWTM does not display new alarms or events in the table (unless you apply a filter or edit your preferences). When the table is resumed, all new alarms or events since the table was paused are added to the display. If alarms or events are deleted while the table is paused, they are not removed from the table. Instead, they are dimmed and cannot be acknowledged or edited. Deleted alarms or events are removed from the table when you resume the table.
 Acknowledge	Makes the chosen alarms or events acknowledged.
 Unacknowledge	Makes the chosen alarms or events unacknowledged.
 Clear	Clears the chosen alarms in the Active Alarms table. When you clear an alarm, the alarm no longer affects the severity of the object (its severity changes to normal), but the alarm remains visible in the Active Alarms table. This option is not available for events.
 Delete	Deletes the chosen alarms or events. When you delete an alarm or event, you remove it from the table, and the MWTM archives the alarm or event in its database. Also, the alarm or event no longer affects the severity of the object.
 Clear and Delete	Clears the chosen alarms and also deletes them from the Active Alarms table. Use the Clear and Delete button if you need to designate an alarm as manually cleared before deleting it. When you use the Clear and Delete button, the MWTM changes the alarm severity of the object to normal, sends an alarm log message to <code>/opt/CSCOs/gm/logs/messageLog.txt</code>, and sends a trap to a northbound host to indicate that the alarm cleared. This option is not available for events.
 Event Properties	Opens the Alarm and Event Properties window, Properties tab.
 Events for Alarm	Launches a dialog that shows a table of events that are associated with the selected alarm. (This button is only available in alarm tables.)
 Edit Notes	Opens the Alarm and Event Properties window, Notes tab.
 Time Difference	Shows the time difference in days, minutes, hours, and seconds between two alarms or events. In the client interface, use the Ctrl key to select two alarms or events. In the web interface, check the check boxes of two alarms or events. Then click the Time Difference button.

Button	Description
 Find (Client interface only)	Finds specified text in the Active Alarms or Event History table.
 Create Sound Filter (Client interface only)	Opens the Event Sound Filters dialog box, with fields populated based on the chosen event.
 Adjust Row Height (Client interface only)	Adjusts the table row height and wraps the message text. Click: - Once to double the row height and wrap the message text. - Again to triple the row height and wrap the message text. - Again for single row height and no message text wrapping. This is the default setting. This setting is saved automatically with your preferences.
 Help for Event	Shows context-sensitive help for the chosen alarm or event in a separate browser window.

Right-click Menus

In the MWTM client interface navigation tree, to display the right-click menu for all:

- Alarms, right-click Active Alarms (see [Right-Click Menu for All Alarms and Events, page 9-16](#)).
- Events, right-click Event History (see [Right-Click Menu for All Alarms and Events, page 9-16](#)).

In the MWTM client interface, to display the right-click menu for a specific alarm or event, right-click the alarm or event in the right pane (see [Right-Click Menu for a Specific Alarm or Event, page 9-17](#)).



Note

Right-click menus are available only in the MWTM client interface.

Right-Click Menu for All Alarms and Events

To see the right-click menu for all active alarms, in the MWTM client interface, select Active Alarms or Event History in the navigation tree and right-click the mouse button.

Menu Command	Description
Show In New Window	Opens the Active Alarms or Event History window in a new window.
Back > <i>List of Windows</i>	Navigates back to a window viewed in this session. The MWTM maintains a list of up to 10 Back windows.
Forward > <i>List of Windows</i>	Navigates forward to a window viewed in this session. The MWTM maintains a list of up to 10 Forward windows.

Right-Click Menu for a Specific Alarm or Event

To see this menu, in the MWTM client interface, select an alarm or event and right-click the mouse button.

The right-click menu provides these options:

Menu Command	Description
Edit Notes	Opens the Edit Alarm and Event Notes dialog for the chosen alarm or event.
Go To > <i>Object</i>	Shows the window for the object associated with the chosen alarm or event. If no object is associated with the alarm or event, this option is not visible.
Change Severity	Changes the alarm severity to critical, major, minor, warning, informational, indeterminate, or normal. Note This right-click menu option appears only in the Active Alarms window.
Acknowledge	Makes the chosen alarms or events acknowledged.
Unacknowledge	Makes the chosen alarms or events unacknowledged.
Clear	Clears the chosen alarm in the Active Alarms table. When you clear an alarm, the alarm no longer affects the severity of the object (its severity changes to normal). The alarm remains visible in the Active Alarms table for 24 hours. After 24 hours, the MWTM archives the alarm in its database. This option is not available for events. Note This right-click menu option appears only in the Active Alarms window.
Delete	Deletes the chosen alarm or event. When you delete an alarm or event, you remove it from the table, and the MWTM archives the alarm or event in its database. Also, the alarm or event no longer affects the severity of the object.
Clear and Delete	Clears the chosen alarm and also deletes it from the Active Alarms table. Use the Clear and Delete button if you need to designate an alarm as manually cleared before deleting it. When you use the Clear and Delete button, the MWTM changes the alarm severity of the object to normal, sends an alarm log message to <code>/opt/CSCOs/gm/logs/messageLog.txt</code> , and sends a trap to a northbound host to indicate that the alarm cleared. This option is not available for events. Note This right-click menu option appears only in the Active Alarms window.
Properties	Opens the Alarm and Event Properties dialog.
Create Sound Filter	Opens the Event Sound Filters dialog box, with fields populated based on the chosen event.
Help for Event	Shows context-sensitive help for the chosen event in a separate browser window.

Managing Filters for Alarms and Events

You can use the MWTM to create filters to customize the information visible for events and alarms.

- [Setting an Alarm or Event Filter, page 9-18](#)

- [Loading an Existing Filter, page 9-25](#)
- [Saving a Filter File, page 9-26](#)

Setting an Alarm or Event Filter

You can use the MWTM Alarm and Event Filter dialog box to change the way alarm or event information appears.

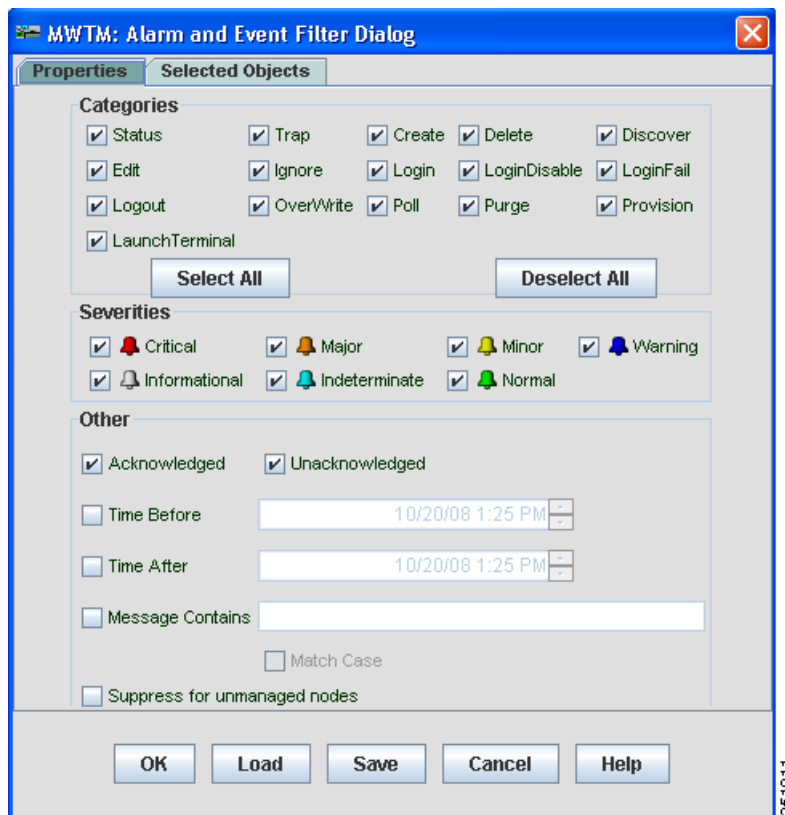


Note

You can access the Alarm and Event Filter dialog box through the client interface or the web interface. Minor differences that exist are noted in this section.

To change the way the MWTM presents event information, click **Event History** in the navigation tree, then click the Set Filter tool  at the top of the Event History window. The Alarm and Event Filter dialog box appears (in the client interface, the window appears with the Properties tab chosen).

Figure 9-6 Alarm and Event Filter Dialog, Showing Event Properties



Note

The Selected Objects tab is available only in the client interface.

For more information about the Alarm and Event Filter dialog box, see these sections:

- [Alarm and Event Filter Buttons, page 9-19](#)

- [Properties Settings, page 9-19](#)
- [Selected Objects Settings, page 9-21](#)
- [Event Filter Example, page 9-25](#)

Related Topics:

- [Loading an Existing Filter, page 9-25](#)
- [Saving a Filter File, page 9-26](#)
- [Viewing Properties for Alarms and Events, page 9-27](#)

Alarm and Event Filter Buttons

The Alarm and Event Filter dialog box contains:

Button	Description
Select All	Checks all check boxes in the section.
Deselect All	Unchecks all check boxes in the section.
OK	Applies any changes you made to the filter and closes the Alarm and Event Filter dialog box.
Load	Opens the Load File Dialog, which you use to load an already existing filter file. If you are viewing events for a specific object in the navigation tree of the MWTM main window, this button is not available.
Save	Opens the Save File Dialog, which you use to save the filter file with a new name, or overwrite an existing filter file. If you are viewing events for a specific object in the navigation tree of the MWTM main window, this button is not available.
Cancel	Closes the Alarm and Event Filter dialog box without applying any changes to the filter.
Help	Shows online help for the current dialog box.

Properties Settings

You use the Properties settings in the Alarm and Event Filter dialog box to specify the types of alarms or events the MWTM should display in the Active Alarms or Event History window, including the category and severity of the alarm or event.

To display the Properties settings, click the Properties tab in the Alarm and Event Filter dialog box.

The Properties tab contains these panes:

- [Categories, page 9-19](#)
- [Severities, page 9-20](#)
- [Other, page 9-21](#)

Categories

Use the Categories pane of the Properties tab to specify which event categories you want to display in the Active Alarms or Event History window.

The following categories are available:

- Status
- Trap
- Create
- Delete
- Discover
- Edit
- Ignore
- Login
- LoginDisable
- LoginFail
- Logout
- OverWrite
- Poll
- Purge
- Provision
- LaunchTerminal

All categories are checked by default. You can click Deselect All, or Select All.


Note

These are the default categories; there might be additional categories that the MWTM system administrator defines. For information about custom categories, see [Changing Event Categories, page 9-41](#).

Severities

Use the Severities pane of the Properties tab to specify which alarm/event severities you want to display in the Active Alarms or Event History window.

The Severities pane contains these default fields:

Check box	Description
Informational	Indicates whether events of the specified severity appear in the Active Alarms/Event History window.
Normal	
Indeterminate	Check boxes are checked by default.
Warning	
Critical	
Minor	
Major	

Other

Use the Other pane of the Properties tab to further define the filter for the Active Alarms or Event History window. These settings are applied to all alarm/event displays in the current view.

Field	Description
Acknowledged	Check box indicating whether only acknowledged alarms/events appear in the Active Alarms/Event History window. This check box is unchecked by default.
Unacknowledged	Check box indicating whether only unacknowledged alarms/events appear in the Active Alarms/Event History window. This check box is checked by default.
Time Before	Check box indicating whether only alarms/events that the MWTM logs prior to a specified date and time appear in the Active Alarms/Event History window. This check box is unchecked by default.
Time Before	Specifies the date and time prior to which alarms/events that the MWTM logs appear in the Active Alarms/Event History window. This field is dimmed unless the Time Before check box is checked.
Time After	Check box indicating whether only alarms/events that the MWTM logs after a specified date and time appear in the Active Alarms/Event History window. This check box is unchecked by default.
Time After	Specifies the date and time after which alarms/events that the MWTM logs appear in the Active Alarms/Event History window. This field is dimmed unless the Time After check box is checked.
Message Contains	Check box indicating whether only alarms/events that contain the specified message text appear in the Active Alarms/Event History window. This check box is unchecked by default.
Match Case	Check box indicating whether only alarms/events that match the case of the text in the Message Contains field appear in the Active Alarms/Event History window. This field is dimmed unless the Message Contains check box is checked. If the Message Contains check box is checked, the default setting for this check box is unchecked.
Suppress for unmanaged nodes	Check box for suppressing alarms/events for any objects that have been set to the unmanaged state (see Unmanaging and Managing Nodes or ITP Signaling Points, page 6-42 , for steps to set an object to the unmanaged state). To suppress alarms/events for unmanaged objects, check the check box. To retain alarms/events for unmanaged objects, uncheck the check box. If you are viewing alarms/events for a specific object in the navigation tree of the MWTM main window, this button is not available.

Selected Objects Settings



Note

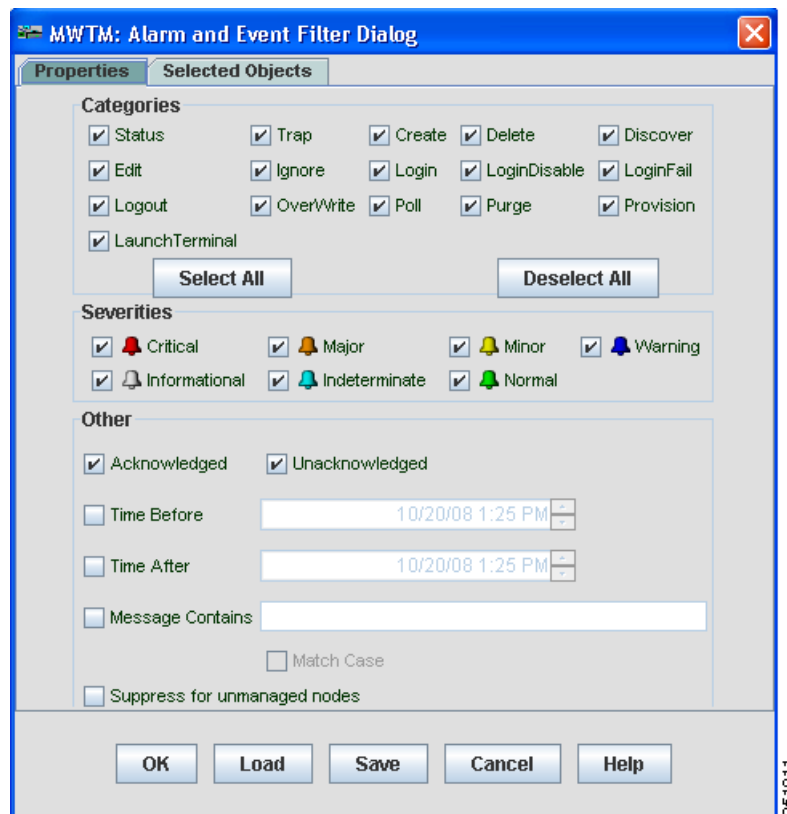
The Selected Objects tab is not available in the Events dialog box if you are viewing events:

- For a specific object in the navigation tree of the MWTM main window.
- Using the web interface.

To specify an object for which the MWTM should display alarms or events in the Active Alarms/Event History window:

-
- Step 1** Click **Active Alarms** or **Event History** or in the navigation tree.
The Active Alarms or Event History window appears in the right pane.
- Step 2** Click the Set Filter tool  at the top of the window.
The Alarm and Event Filter dialog box appears with the Properties tab chosen.
- Step 3** Click the **Selected Objects** tab.
The Alarm and Event Filter dialog box appears with the Selected Objects tab highlighted.
-

Figure 9-7 Event Filter Dialog, Showing Event Selected Objects



The Selected Objects settings contains:

Field or Button	Description
Node	Drop-down list box of all nodes that the MWTM has discovered. If you: - Want to filter alarms/events based on a node, select a node from the drop-down list box. - Do not want to filter alarms/events based on a node, select None. The MWTM grays-out the other object fields. This is the default setting.
ApplicationServerProcess (ITP only)	Drop-down list box of all application server processes associated with the chosen node: - If you want to filter alarms/events based on an application server process, select an application server process from the drop-down list box. - If you do not want to filter alarms/events based on an application server process, select None. This is the default setting.
SignalingGatewayMatedPair (ITP only)	Drop-down list box of all signaling gateway-mated pairs associated with the chosen node: - If you want to filter alarms/events based on a signaling gateway-mated pair, select a signaling gateway-mated pair from the drop-down list box. - If you do not want to filter alarms/events based on a signaling gateway-mated pair, select None. This is the default setting.
SignalingPoint (ITP only)	Drop-down list box of all signaling points associated with the chosen node: - If you want to filter alarms/events based on a signaling point, select a signaling point from the drop-down list box. - If you do not want to filter alarms/events based on a signaling point, select None. This is the default setting.
Linkset (ITP only)	Drop-down list box of all linksets associated with the chosen signaling point: - If you want to filter alarms/events based on a linkset, select a linkset from the drop-down list box. - If you do not want to filter alarms/events based on a linkset, select None. This is the default setting.
Link (ITP only)	Drop-down list box of all links associated with the chosen linkset: - If you want to filter alarms/events based on a link, select a link from the drop-down list box. - If you do not want to filter alarms/events based on a link, select None. This is the default setting.

Field or Button	Description
ApplicationServer (ITP only)	Drop-down list box of all application servers associated with the chosen signaling point: - If you want to filter alarms/events based on an application server, select an application server from the drop-down list box. - If you do not want to filter alarms/events based on an application server, select None. This is the default setting.
ApplicationServerProcess Association (ITP only)	Drop-down list box of all application server process associations associated with the chosen application server: - If you want to filter alarms/events based on an application server process association, select an application server process association from the drop-down list box. - If you do not want to filter alarms/events based on an application server process association, select None. This is the default setting.
Card (RAN-O only)	Drop-down list box of all cards associated with the chosen node: - If you want to filter alarms/events based on a card, select a card from the drop-down list box. - If you do not want to filter alarms/events based on a card, select None. This is the default setting.
Interface	Drop-down list box of all interfaces (including subinterfaces) associated with the chosen node or card: - If you want to filter alarms/events based on an interface, select an interface from the drop-down list box. - If you do not want to filter alarms/events based on an interface, select None. This is the default setting.
Backhaul (RAN-O only)	Drop-down list box of all RAN backhauls associated with the chosen node or card: - If you want to filter alarms/events based on an interface, select an interface from the drop-down list box. - If you do not want to filter alarms/events based on an interface, select None. This is the default setting.
Selected Objects: Object Type	Indicates the type of object, if any, on which the filter is based.
Selected Objects: AS (ITP only)	Indicates the application server, if any, on which the filter is based.
Selected Objects: ASP (ITP only)	Indicates the application server process, if any, on which the filter is based.
Selected Objects: ASPA (ITP only)	Indicates the application server process application, if any, on which the filter is based.
Selected Objects: Link (ITP only)	Indicates the link, if any, on which the filter is based.
Selected Objects: Linkset (ITP only)	Indicates the linkset, if any, on which the filter is based.
Selected Objects: Node	Indicates the node, if any, on which the filter is based.

Field or Button	Description
Selected Objects: SGMP (ITP only)	Indicates the signaling gateway-mated pair, if any, on which the filter is based.
Selected Objects: SP (ITP only)	Indicates the signaling point, if any, on which the filter is based.
Selected Objects: Card (RAN-O only)	Indicates the card, if any, on which the filter is based.
Selected Objects: Interface	Indicates the interface or subinterface, if any, on which the filter is based.
Selected Objects: Backhaul (RAN-O only)	Indicates the RAN backhaul, if any, on which the filter is based.

Event Filter Example

This example shows how to set an event filter to display trap messages for warning events for a specific node. You perform this procedure by using the MWTM client interface.

-
- Step 1** Choose **Event History** in the navigation tree of the MWTM main window of the client interface.
- Step 2** Click the Event Filter tool  at the top of the Event History window.
The Event Filter dialog box appears with the Properties tab chosen.
- Step 3** In the Categories pane, uncheck all check boxes except for the Trap check box.
- Step 4** In the Severities pane, uncheck all check boxes except for the Warning check box.
- Step 5** Click the Selected Objects tab.
- Step 6** In the drop-down list box, choose a node from the list of discovered nodes.
- Step 7** To activate the event filter and close the Event Filter dialog box, click **OK**.
- Step 8** To save the event filter for future use:
- In the Event Filter dialog box, click **Save**. This action opens the Save Filter dialog box.
 - In the Save Filter dialog box, enter a meaningful name in the Filename text box (for example, Node109-WarningTraps).
 - Click **OK** to close the Save Filter dialog box.
 - Click **OK** to close the Event Filter dialog box.
- In the future, to view traps for warning events for Node109, click **Load** in the Event Filter dialog box, choose the Node109-WarningTraps filter, then click **OK**. The Events window will only display warning traps for Node109 until you load a different event filter or change the current one.
-

Loading an Existing Filter

You use the MWTM client interface to load a specific filter file and change the list of filter files.

To load an existing filter, click **Load** in the Alarm and Event Filter dialog box. The Load File Dialog: Load Filter dialog box appears.

The Load File Dialog: Load Filter contains:

Field or Button or Icon	Description
Type	Icon indicating whether the item in the table is a file or a folder.
Name	Name of the filter file or folder.
Last Modified	Date and time the filter file or folder was last modified.
Size (bytes)	Size of the filter file or folder, in bytes.
Number of Files (appears in lower left corner)	Total number of filter files and folders.
OK	Loads the chosen filter, saves any changes you made to the list of files, and closes the dialog box. To load an filter file, double-click it in the list, select it in the list and click OK , or enter the name of the file and click OK . The MWTM loads the filter file, saves any changes you made to the list of files, closes the Load File Dialog: Load Filter dialog box, and returns to the Alarm and Event Filter dialog box.
Delete	Deletes the chosen file from the filter file list. The MWTM issues an informational message containing the name and location of the deleted file.
Cancel	Closes the dialog box without loading an filter file or saving any changes to the filter file list.
Help	Shows online help for the dialog box.

Saving a Filter File

You use the MWTM client interface to save a specific filter file and change the list of filter files.

When you are satisfied with the filter settings, click **Save** in the Alarm and Event Filter dialog box. The Save File Dialog:Save Filter dialog box appears.

The Save File Dialog: Save Filter contains:

Field or Button or Icon	Description
Type	Icon indicating whether the item in the table is a file or a folder.
Name	Name of the filter file or folder.
Last Modified	Date and time the filter file or folder was last modified.
Size (bytes)	Size of the filter file or folder, in bytes.
Filename	Name by which you want to save the filter file. If you create a new filter filename, you can use any letters, numbers, or characters in the name that are allowed by your operating system. However, if you include any spaces in the new name, the MWTM converts those spaces to dashes. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i> .

Field or Button or Icon	Description
Number of Files (visible in bottom left corner)	Total number of filter files and folders.
OK	Saves any changes you made to the current filter file and closes the dialog box. To save the filter file with a new name, use one of these procedures. To save the file with: - A completely new name, enter the new name and click OK. - An existing name, overwriting an old filter file, select the name in the list and click OK. The MWTM saves the filter file with the new name, saves any changes you made to the list of files, closes the Save File Dialog: Save Filter dialog box, and returns to the Alarm and Event Filter dialog box.
Delete	Deletes the chosen file from the filter file list. The MWTM issues an informational message containing the name and location of the deleted file.
Cancel	Closes the dialog box without saving the filter file or saving any changes to the filter file list.
Help	Shows online help for the dialog box.

Viewing Properties for Alarms and Events

You use the MWTM to view detailed information about a chosen alarm or event, including its associated object, status, and other information.

To view detailed information about an alarm or event, in the:

- MWTM client interface, right-click the alarm or event in a window, then select **Event Properties** in the right-click menu.
- Web interface, select an alarm or event by checking its check box, then click the **Event Properties** icon  in the toolbar.

The Event Properties dialog box appears. The Event Properties dialog box contains:

Tab, Field, or Button	Description
Properties	Tab that shows detailed information about the chosen alarm or event.
Message	Message text for the alarm or event. You can customize this field (see Changing the Way the MWTM Processes Events, page 9-35).

Tab, Field, or Button	Description
Category	Type of the alarm or event. Default values are: • Create—Creation event, such as the creation of a seed file. • Delete—Deletion event, such as the deletion of an object or file. • Discover—Discovery event, such as Discovery beginning. • Edit—Edit event. A user has edited an object. • Ignore—Ignore event. A user has ignored a link or linkset. • Login—Login event. A user has logged in to the MWTM. • LoginDisable—LoginDisable event. The MWTM has disabled a user's User-Based Access authentication as a result of too many failed attempts to log in to the MWTM. • LoginFail—LoginFail event. A user's attempt to log in to the MWTM has failed. • Logout—Logout event. A user has logged out of the MWTM.
Category (continued)	• OverWrite—OverWrite event. An existing file, such as a seed file or route file, has been overwritten. • Poll—Poll event, such as an SNMP poll. • Purge—Purge event. A user has requested Discovery with Delete Existing Data selected, and the MWTM has deleted the existing MWTM database. • Status—Status change message generated. • Trap—SNMP trap message generated. You can customize this field (see Changing Event Categories, page 9-41).
Severity	Severity of the alarm or event. Possible severities are:  Critical  Major  Minor  Warning  Normal  Indeterminate  Informational You can customize this field (see Right-Click Menu for a Specific Alarm or Event, page 9-17).
Original Severity	Original severity of the alarm or event.
Create Time	Date and time the event was logged.
Change Time	Date and time the alarm last changed. Note This field is important only for alarms.
Acknowledged	Indicates whether the alarm or event has been acknowledged.
Acknowledged By	Name of the node that last acknowledged the alarm or event. If no one has acknowledged the alarm or event, this field is not shown.

Tab, Field, or Button	Description
Internal ID	An internal identification that the MWTM uses for the alarm or event.
Event Name	The name for the alarm or event, for example, InterfaceState.
Count	Number of times this alarm occurred. Note This field is important only for alarms because an event count will always be 1.
Element Name	Name of the managed element, for example, the node name.
object name	Name of the object associated with the alarm or event. The object can be: • Node or Interface • ITP objects: SP, Linkset, Link, AS, ASP, ASPA, SGMP • RAN-O objects: RAN Backhaul, Card • APN objects are applicable for GGSN
Notes	Tab that shows notes associated with this alarm or event. If no note is currently associated with this alarm or event, this field shows the value <i>No Notes</i> .
Last Updated	In the Notes tab, the date and time the Notes field for this alarm or event was last updated. If no note is currently associated with this alarm or event, this field shows the value <i>Not Set</i> .
Details	Tab that shows specific alarm or event attributes.
Close	Closes the Event Properties dialog box.

Attaching a Note to an Alarm or Event

You use the MWTM to annotate an alarm or event, attaching a descriptive string to it.

To annotate an alarm or event in the:

- MWTM client, right-click an alarm or event in the Event History window, then select **Edit Notes** in the right-click menu. The Edit Event dialog box appears.
- Web interface, select an alarm or event in the Event History window by checking its check box, then click the **Edit Notes** icon . The Event Properties dialog box appears, with the Notes tab chosen.



Note

You can add a note to an alarm or event by using either the MWTM client or the web interface. You can also view the note from either interface.

The Edit Event Dialog contains:

Field or Button	Description
Name	Message text of the alarm or event.
Last Update	Date and time the Notes field for this alarm or event was last updated. If no note is currently associated with this alarm or event, this field shows the value <i>Not Set</i> . You cannot edit this field.

Field or Button	Description
Notes	Notes to associate with this alarm or event. In this field, you can enter any important information about the alarm or event, such as its associated object, what triggered the alarm or event, how often it has occurred, and so on.
Edit	Enables you to edit or add a note.
Save	Saves changes you have made to the alarm or event information.
Cancel	Cancels the operation without saving any changes.
Help	Shows online help for the current window.

Related Topics:

[Viewing Properties for Alarms and Events, page 9-27](#)

Viewing Archived Event Files on the Web

The All Network Event Archived Files page provides access to archived alarm and event files for the server to which you are connected.

To access archived event files:

-
- Step 1** In a web browser, navigate to the MWTM web interface (for details, see [Accessing the MWTM Web Interface, page 11-1](#)).
- Step 2** Choose **File Archive > Events** from the web navigation tree.
In the Last Modified Date column, choose the day you want to view archived event files for.
- Step 3** Adjacent to the date you have chosen, click the **Status Changes and SNMP Traps** link under **View**. The Network Status Archive page appears, showing a list of the status and trap messages in the archive.
-

Viewing the Event Metrics Report on the Web

The Event Metrics Report page shows a number of metrics for the MWTM, based on the number of messages of each type and severity that the MWTM receives.

To view the event metrics report using the MWTM Web interface:

-
- Step 1** In a web browser, navigate to the MWTM web interface (for details, see [Accessing the MWTM Web Interface, page 11-1](#)).
- Step 2** Click **Reports > Statistics > Events**, or from the Reports page, click **Events**.
-

The Event Metrics Report page contains the following tables:

- [Message Types Table, page 9-31](#)
- [Message Severity Table, page 9-31](#)
- [Status Messages Table, page 9-32](#)

- [Trap Messages Table, page 9-33](#)
- [Messages/Day Table, page 9-33](#)
- [Status Change Messages/Day Table, page 9-34](#)
- [SNMP Trap Messages/Day Table, page 9-34](#)
- [Files Processed Table, page 9-34](#)
- [Date Range Table, page 9-34](#)

Message Types Table

The Message Types table contains the following columns:

Column	Description
Message Types	Total number of messages of each type that the MWTM received. Possible types are: • Total Messages—Total number of messages of all types • Total Status—Total number of status change messages • Total Traps—Total number of SNMP trap messages
Num	Number of messages of each type that the MWTM received.
Num/Total	Number of messages of a given type that the MWTM received, divided by the total number of messages that the MWTM received, shown as a percentage.

Message Severity Table

The Message Severity table contains the following columns:

Column	Description
Message Severity	Total number of messages (status change messages and SNMP trap messages) of each severity that the MWTM received: • Total Warning • Total Normal • Total Unclass • Total Minor • Total Major • Total Informational • Total Error • Total Critical • Total Admin
Num	Number of messages of each severity that the MWTM received.
Num/Total	Number of messages of a given severity that the MWTM received, divided by the total number of messages that the MWTM received, shown as a percentage.

Status Messages Table

The Status Messages table contains the following columns:

Column	Description
Status Messages	Total number of status change messages of each severity that the MWTM received. Possible severities are: • Status Minor • Status Normal • Status Major • Status Warning • Status Informational • Status Critical • Status Unclass • Status Error • Status Admin
Num	Number of status change messages of each severity that the MWTM received.
Num/Status	Number of status change messages of a given severity that the MWTM received, divided by the total number of status change messages that the MWTM received, shown as a percentage.
Num/Total	Number of status change messages of a given severity that the MWTM received, divided by the total number of messages (status change messages and SNMP trap messages) that the MWTM received, shown as a percentage.

Trap Messages Table

The Trap Messages table contains the following columns:

Column	Description
Trap Messages	Total number of SNMP trap messages of each severity that the MWTM received. Possible severities are: • Trap Warning • Trap Unclass • Trap Normal • Trap Minor • Trap Major • Trap Informational • Trap Error • Trap Critical • Trap Admin
Num	Number of SNMP trap messages of each severity that the MWTM received.
Num/Trap	Number of SNMP trap messages of a given severity that the MWTM received, divided by the total number of SNMP trap messages that the MWTM received, shown as a percentage.
Num/Total	Number of SNMP trap messages of a given severity received by the MWT, divided by the total number of messages (status change messages and SNMP trap messages) that the MWTM received, shown as a percentage.

Messages/Day Table

The Messages/Day table contains the following columns:

Column	Description
Day	Date for which metrics are calculated.
NumMsgs	Total number of messages that the MWTM received on a given day.
NumMsgs/TotalMsgs	Number of messages that the MWTM received on a given day, divided by the total number of messages (status change messages and SNMP trap messages) that the MWTM received on all days, shown as a percentage.

Status Change Messages/Day Table

The Status Change Messages/Day table contains the following columns:

Column	Description
Day	Date for which metrics are calculated.
NumStatMsgs	Total number of status change messages that the MWTM received on a given day.
NumStatMsgs/TotalMsgs	Number of status change messages that the MWTM received on a given day, divided by the total number of messages (status change messages and SNMP trap messages) that the MWTM received on all days, shown as a percentage.
NumStatMsgs/TotalStatMsgs	Number of status change messages that the MWTM received on a given day, divided by the total number of status change messages that the MWTM received on all days, shown as a percentage.

SNMP Trap Messages/Day Table

The Status Change Messages/Day table contains the following columns:

Column	Description
Day	Date for which metrics are calculated.
NumTrapMsgs	Total number of SNMP trap messages that the MWTM received on a given day.
NumTrapMsgs/TotalMsgs	Number of SNMP trap messages that the MWTM received on a given day, divided by the total number of messages (status change messages and SNMP trap messages) that the MWTM received on all days, shown as a percentage.
NumTrapMsgs/TotalTrapMsgs	Number of SNMP trap messages that the MWTM received on a given day, divided by the total number of SNMP trap messages that the MWTM received on all days, shown as a percentage.

Files Processed Table

The Files Processed table lists all files that the MWTM has processed.

Date Range Table

The Date Range table displays the date and time when the MWTM began collecting metrics, and the date and time of the most recent metrics.

Changing the Way the MWTM Processes Events

The three types of MWTM events are:

- **Trap events**—Incoming events that the MWTM does not solicit
- **Status events**—Status changes that the MWTM detects
- **User Action events**—Events that user actions trigger

In those broad types, there occur subordinate types of events, each with a default category, severity, color, message text, and event help file. You use the MWTM to change the default characteristics of each type of event, tailoring them to meet your needs.



Note

Changes you make to the MWTM event processing can adversely affect your operating environment. In most environments, the MWTM recommends that you use the default event-processing settings without modification.

To change the MWTM event processing, use one of these procedures:

- Choose **Tools > Event Editor** from the MWTM main menu of the client interface
- Choose **Start > Programs > Cisco MWTM Client > MWTM Event Editor** in Windows.
- Enter the `mwtm eventeditor` command (see [mwtm eventeditor](#), page B-28).

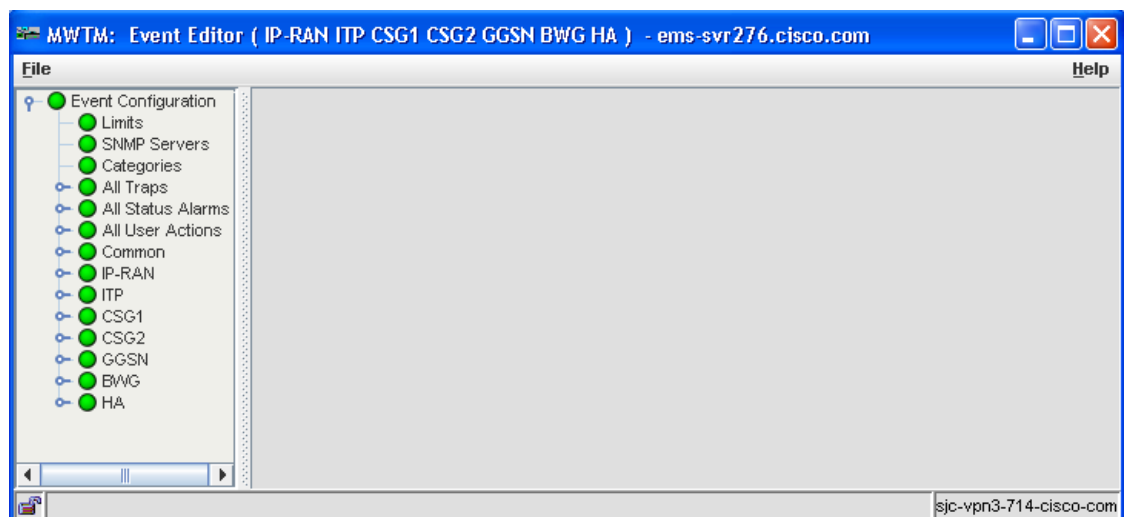
The MWTM launches the MWTM Event Editor in the client interface. The Event Editor is not available in the web interface.



Note

To use the Event Editor, you must be a power user (level 2) or higher.

Figure 9-8 *MWTM Event Editor*



You use the Event Editor to customize the visible category, severity, color, and message associated with events; and load, save, and deploy customized event configurations. You can also specify a list of SNMP servers to which the MWTM should forward events in the form of traps.

The high-level MWTM event processing settings appear in the navigation tree in the left pane in the MWTM Event Editor window. The detailed settings for each high-level setting appear in the content area in the right pane.

The MWTM Event Editor menu provides these options:

Menu Command	Description
File > Load Draft	Loads the local copy of the event configuration that you saved.
File > Save Draft (Ctrl-S)	Saves a local copy of the event configuration, including any changes you made by using the Event Editor. You can save only one local copy of the event configuration. You cannot specify a filename for the local copy.
File > Load Default	Loads the default event configuration on this MWTM client. The default event configuration is the standard event configuration that the MWTM uses when it is first installed. The default event configuration stored on the MWTM server and shared by all MWTM clients, but the clients cannot modify it.
File > Load Running	Loads the event configuration that is currently running on the MWTM server.
File > Load Backup	Loads the backup event configuration from the MWTM server. The MWTM creates a backup event configuration every time the event configuration on the MWTM server is overwritten.
File > Revert	Reverts to the last event configuration that was loaded on the MWTM client. This could be the draft, default, running, or backup event configuration.
File > Deploy	Deploys the event configuration that is currently being edited on this MWTM client to the MWTM server. The deployed event configuration does not take effect until you restart the MWTM server. When you restart the MWTM server, the MWTM automatically reflects your changes to the event configuration on the MWTM server and on all MWTM clients that connect to that server, and reflects any new or changed categories, severities, and other event characteristics in its web navigation bars.
File > Exit	Closes the Event Editor window. If you have made any changes to the event configuration, the MWTM asks if you want to save the changes before leaving the window. Click: • Save Draft to save the changes in a local copy of the event configuration. You can save only one local copy of the event configuration. You cannot specify a filename for the local copy. • Deploy to deploy the event configuration, including any changes you made, to the MWTM server. The deployed event configuration does not take effect until you restart the MWTM server. When you restart the MWTM server, the MWTM automatically reflects your changes to the event configuration on the MWTM server and on all MWTM clients that connect to that server, and reflects any new or changed categories, severities, and other event characteristics in its web display navigation bars. • No or Cancel to close the prompt window and return to the Event Editor window.

Menu Command	Description
Help > Topics (F1)	Shows the table of contents for the MWTM online help.
Help > Window (Shift-F1)	Shows online help for the current window.
Help > About (F3)	Shows build date, version, SSL support, and copyright information about the MWTM application.

This section provides this information:

- [Changing Event Limits, page 9-37](#)
- [Specifying a List of SNMP Servers for Trap Forwarding, page 9-40](#)
- [Changing Event Categories, page 9-41](#)
- [Configuring Trap, Status Alarm, or User Action Events, page 9-42](#)

Changing Event Limits

To change limits for the MWTM event database, click the turner  beside Event Configuration, then click **Limits**. The Limits Configuration window appears in the right pane.

Field	Description
MaxEventDbRecords	Sets the maximum number of events allowed in the in-memory or active database. You can observe these events in the client NBAPI. The MWTM archives deleted events. By default, the active database can hold a maximum of 10,000 events. If the database exceeds 10,000 events, the MWTM archives the oldest events until the database is reduced to 10,000 events. To change the size of the active database, enter the new size, in number of events, in this field. The valid range is 0 events (that is, no limit) to an unlimited number of events. The default setting is 10,000 events. Note As you increase the size of the event database, you negatively impact the performance of the MWTM server and clients.
MaxAlarmDbRecords	Sets the maximum number of alarms allowed in the in-memory or active database. You can observe these alarms in the client NBAPI. The MWTM archives deleted alarms. By default, the active database can hold a maximum of 10,000 alarms. If the database exceeds 10,000 alarms, the MWTM archives the oldest alarms until the database is reduced to 10,000 alarms. To change the size of the active database, enter the new size, in number of alarms, in this field. The valid range is 0 alarms (that is, no limit) to an unlimited number of alarms. The default setting is 10,000 alarms. Note As you increase the size of the alarm database, you negatively impact the performance of the MWTM server and clients.

Field	Description
MaxEventTimeToLive	Sets the maximum length of time, in days, the MWTM should retain events in the in-memory or active database. You can observe these events in the client NBAPI. The MWTM archives deleted events. By default, the active database retains events a maximum of 7 days. The MWTM archives events that are older than 7 days. To change the maximum age for events, enter the new age, in days, in this field. The valid range is 0 days (events are purged at each maintenance interval) to an unlimited number of days. The default setting is 7 days.
CompressEventDbInterval	Sets the length of time, in minutes, between maintenance checks of the in-memory or active database. The MWTM archives these events and alarms when this task runs. Also, the oldest archived events and alarms may be deleted from the database. By default, the MWTM performs maintenance on the active database every 15 minutes, archiving all events and alarms in excess of 10,000, all events older than 7 days, and all alarms older than 14 days. To change the maintenance interval, enter the new interval, in minutes, in this field. The valid range is 0 minutes (perform continual maintenance; not advised) to an unlimited number of minutes. The default setting is 60 minutes. Note The smaller the maintenance interval, the greater the negative impact on the performance of the MWTM server and clients.
AutomationTimeout	Sets the maximum length of time, in seconds, the MWTM should allow an event automation script to run. By default, the MWTM event database allows an event automation script to run for 300 seconds (5 minutes) before canceling the script and moving on. To change the event automation timeout interval, enter the new interval, in seconds, in this field. The valid range is 0 seconds (no automation) to an unlimited number of seconds. The default setting is 300 seconds. Note The MWTM runs each automation script sequentially, not in parallel. Therefore, the longer the automation timeout interval, the greater the chance that a failed script can delay subsequent scripts.
ProcessUndiscovered	Determines whether the MWTM should process events from undiscovered nodes: • False—Do not process events from undiscovered nodes. This setting is the default. • True—Begin processing events from undiscovered nodes.

Send Updates	Determines whether the MWTM should send traps northbound: • False—Do not send traps northbound when an event is updated or deleted. Only send traps when an event is new. This setting is the default. • True—(Default setting) Send traps northbound when an event is updated, deleted, or new.
ProcessUnrecognizedTraps	Determines whether the MWTM should create events for unrecognized traps: • False—Do not create events for unrecognized traps. • True—(Default setting) Create events for unrecognized traps.
TrapGenThrottle	A delay (in milliseconds) between each trap sent to a northbound host. This value is helpful if the MWTM is sending traps faster than the northbound host can receive them. The default is 10 milliseconds.

Field	Description
AllowStateAggregation	 Caution This feature is for advanced users (Cisco developers and third-party integrators). Determines whether the MWTM should allow alarms to change the state of the node: • False—Alarms will not affect the node state. • True—Alarms will affect the node state. This setting is the default.
ClearedAlarmsTimetoLive	The time, in minutes, before the MWTM archives cleared alarms. The default setting is 1440 minutes (24 hours).
SendEvents	Determines whether the MWTM should send events to a northbound system: • False—(Default setting) Does not send events to the northbound system. • True—Sends events to the northbound system.
SendAlarms	Determines whether the MWTM should send alarms to a northbound system: • False—Does not send alarms to the northbound system. • True—(Default setting) Sends alarms to the northbound system.
UseAlternateTrapOids	When set to true, allows user-specified trap OIDs (SNMPv1 trap enterprise/specific type or SNMPv2 snmpTrapOID)
ClearAlarmsOnUpdate	When set to true, automatically clears outstanding alarms when a new event in the alarm sequence occurs.
DeleteAlarmsOnUpdate	When set to true, automatically deletes outstanding alarms when a new event in the alarm sequence occurs.
SendAlarmSetsAndClears	When set to true, sends a northbound notification only when an alarm is raised and when it is cleared.
ArchiveActiveAlarms	Determines whether the MWTM should archive alarms. • True—(Default setting) Allows alarm archiving in accordance with both MaxAlarmAge and MaxAlarmDbRecords. • False. Ignore MaxAlarmAge—Does not archive alarms until they are manually or automatically cleared through alarm correlation. • False. Ignore MaxAlarmAge and MaxAlarmDbRecords—Never automatically archive an active alarm.

Specifying a List of SNMP Servers for Trap Forwarding

You use the MWTM to specify a list of SNMP servers, or hosts, to which the MWTM should forward events in the form of traps.

For more information about enabling MWTM trap forwarding, see [Forwarding Events as Traps to Other Hosts, page 9-48](#).

To specify the list of hosts, click the turner  beside Event Configuration, then click **SNMP Servers**. The SNMP Servers Configuration window appears in the content area in the right pane.

Field or Button	Description
Host	Name of the host NMS that should receive traps from the MWTM. The host must be IP-routable, and the name must be a valid IP address or DNS name.
Port	Host port number to which the MWTM should forward traps.
Community	SNMP community string that the MWTM should include in forwarded traps.
Version	Trap version to forward. Valid values are 1 and 2c.
Trap Type	Type of trap that the MWTM should forward to this host. Valid trap types are: - CISCO-SYSLOG: The CISCO-SYSLOG-MIB clogMessageGenerated trap. - CISCO-EPM-NOTIFICATION: CISCO-EPM-NOTIFICATION-MIB ciscoEpmNotificationRev1 trap.
Add	Adds a new hostname to the bottom of the list. Type over the default values with the new values.
Delete	Deletes the chosen hostname from the list.
Send a trap for all events	Checks the Send Traps check box for all MWTM events. Click this button if you want the MWTM to forward all events to the list of hosts. If you click this radio button, and then you uncheck even a single Send Traps check box for any event, the MWTM unchecks this button. This radio button is mutually exclusive with the Send a trap for no events button.
Send a trap for no events	Unchecks the Send Traps check box for all MWTM events. Click this button if you do not want the MWTM to forward any events to the list of hosts. This is the default setting. If you click this radio button, and then you check even a single Send Traps check box for any event, the MWTM unchecks this button. This radio button is mutually exclusive with the Send a trap for all events button.

Changing Event Categories

To change categories for the MWTM event database, click the turner  beside Event Configuration, then click **Categories**. The Categories Configuration window appears in the content area in the right pane.

Field or Button	Description
Category Name	Lists the names of the currently defined MWTM event categories. By default, the MWTM provides these event categories: • Status—Status change message generated. • Trap—SNMP trap message generated. • Create—Creation event, such as the creation of a seed file. • Delete—Deletion event, such as the deletion of an object or file.
Category Name (continued)	• Discover—Discovery event, such as Discovery beginning. • Edit—Edit event. A user has edited an event, linkset, or node. • Ignore—Ignore event. A user has Ignored a link or linkset.
Category Name (continued)	• Login—Login event. A user has logged in to the MWTM. • LoginDisable—LoginDisable event. The MWTM has disabled a user's User-Based Access authentication as a result of too many failed attempts to log in to the MWTM. • LoginFail—LoginFail event. An attempt by a user to log in to the MWTM has failed. • Logout—Logout event. A user has logged out of the MWTM. • OverWrite—OverWrite event. An existing file, such as a seed file or route file, has been overwritten. • Poll—Poll event, such as an SNMP poll. • Purge—Purge event. A user has requested Discovery with Delete Existing Data selected, and the MWTM has deleted the existing the MWTM database. To change the name of an existing event category, highlight the category name and type over it with the new name. For example, you could replace every occurrence of LoginFail with BadLogin.
Add	Adds a new category name to the bottom of the list. Type over the default category name with the new name.
Delete	Deletes the chosen category name from the list. If events in the MWTM database use the deleted category name, the Entry Substitution dialog box appears. Use this dialog box to select a new category name in place of the deleted category name. Select an existing category name from the drop-down list box, or enter a new category name. If you enter a new category name, the MWTM adds it to the Category Name field.

Configuring Trap, Status Alarm, or User Action Events

The MWTM can detect these event types:

- **Traps**—Events that are triggered by SNMP traps or notifications
- **Status Alarms**—Events that are triggered by status changes
- **User Actions**—Events that are triggered by user actions

You can choose to view all traps, all status alarms, and all user actions, or you can view these based on network type (RAN-O, ITP, and so on.)

To configure the event parameters for any of these event types:

Step 1 Choose **Tools > Event Editor** from the MWTM main menu in the client interface.

Step 2 Click the turner  beside Event Configuration.

Step 3 Click the turner  beside the event type that you want to configure:

- All Traps
- All Status Alarms
- All User Actions
- Common (lists all traps, status alarms, and user actions common to all networks)
- IPRAN
- ITP
- CSG1
- CSG2
- GGSN
- BWG
- HA

The MWTM lists the currently defined traps, status alarms, or user actions in the navigation tree under the event type.

Step 4 Click the turner  beside the specific trap, status alarm, or user action for which you want to configure an event.

The MWTM lists the currently defined events in the navigation tree under the chosen event type.

Step 5 To add an event to an event type, right-click the event name and select **Add** from the right-click menu.

The MWTM adds the chosen event to the list of configured events and creates a default entry for the event in the left pane.

Step 6 Click the default entry in the left pane.

The Event Configuration pane appears in the right pane.

Step 7 Configure the event by adjusting the parameters.

Step 8 To delete an event, right-click the event in the left pane and click **Delete**.

The Event Configuration pane contains:

Field or Button	Description
Name	Fixed, internal name of the event, such as <code>cItpRouteStateChange</code> . You cannot change this field.
Event Keys and Setting	 Caution This feature is for advanced users (Cisco developers and third-party integrators). Names of the event keys, such as <code>RouteDestinationState</code>, and their settings, such as <code>False</code>. You cannot change the names of the event keys, but you can change their settings. To change an event key setting, select a new setting from the drop-down list box. For example, you can change the setting for <code>RouteDestinationState</code> from <code>Accessible</code> to <code>Unknown</code>.
Category	Category of the event (for example, from <code>Trap</code> to <code>Status</code>). To change the category, select a new category from the drop-down list box.
Severity	Severity of the event (for example, from <code>Warning</code> to <code>Minor</code>). To change the severity, select a new severity from the drop-down list box.
Event Name	User-specified name for the event, that the MWTM uses for trap forwarding, also used in the MWTM client. If you want the MWTM to forward this event in the form of a trap to another host, you can specify a new, more meaningful name for the event. The new name can be from 1 to 30 characters, and can contain any letters (upper- or lowercase), any numbers, and any special characters. If you do not specify a new name, the MWTM uses the default name, <code>MWTM</code>. For more information about trap forwarding, see Forwarding Events as Traps to Other Hosts, page 9-48.
Message	Message text associated with the event. To change the message text, type over the message text. You can also right-click in the field and choose Launch Text Editor, where you can update, clear, or discard your text changes. You can also insert variable text in the message. To do so, right-click in the message text area. A popup menu of the valid substitutions for this event appears. To insert a variable in the text area, select from the popup menu.

Event Name	User-specified name for the event, that the MWTM uses for trap forwarding, also used in the MWTM client.
	If you want the MWTM to forward this event in the form of a trap to another host, you can specify a new, more meaningful name for the event. The new name can be from 1 to 30 characters, and can contain any letters (upper- or lowercase), any numbers, and any special characters. If you do not specify a new name, the MWTM uses the default name, <code>MWTM</code>. For more information about trap forwarding, see Forwarding Events as Traps to Other Hosts, page 9-48.
Message	Message text associated with the event. To change the message text, type over the message text. You can also right-click in the field and choose Launch Text Editor, where you can update, clear, or discard your text changes. You can also insert variable text in the message. To do so, right-click in the message text area. A popup menu of the valid substitutions for this event appears. To insert a variable in the text area, select from the popup menu.

Field or Button	Description
Action: Run	Automation command or script for the event that a UNIX process runs. You use the MWTM to automate events. That is, you can configure the MWTM to call a UNIX script to drive automatic paging or e-mail, for example, whenever the MWTM logs an event for which you have defined an automation script. To configure automation for an event, enter a Run line with this format: <i>UNIXCommand EventParameters</i> where: • <i>UnixCommand</i> specifies either a binary command name or a shell script. • <i>EventParameters</i> are information from the event that the MWTM sends to <i>UnixCommand</i> as parameters. The set of <i>EventParameters</i> is the same as the set of Message element parameters, and they are specified the same way.
Action: Run (continued)	For example, this Run line: <pre>/users/johndoe/auto-inhibit.exp \$NodeDisplayName \$User</pre> causes these automatic actions whenever the MWTM logs the associated event: • The MWTM spawns a UNIX process to execute the <i>/users/johndoe/auto-inhibit.exp</i> script. • The MWTM passes the <i>\$NodeDisplayName</i> and <i>\$User</i> parameters to the script. After you deploy the new event settings and restart the MWTM server, the specified event causes the automation script to run. When configuring automation for events, remember: • Detailed information about event automation scripts, including the times they start and stop and any output produced by the scripts, is recorded in the MWTM system event automation log file (see Viewing the Event Automation Log, page 11-23). • The MWTM event automation scripts run separately from all other MWTM processes. • If the MWTM logs more than one automated event in rapid succession, the MWTM runs each automation script sequentially, not in parallel. The MWTM spawns a new UNIX process for each script, and waits for it to complete before running the next script. • By default, the MWTM allows an event automation script to run for 300 seconds (5 minutes) before canceling the script and moving on to the next script. To change the maximum run-time for event automation scripts, see Changing Event Limits, page 9-37. You can right-click in the field and choose Launch Text Editor, where you can update, clear, or discard your text changes.
Action: Poll (available only for Trap events)	Check box indicating whether MWTM should poll the associated nodes. If you: • Want MWTM to poll the nodes when this event occurs, check the check box. • Do not want MWTM to poll the nodes when this event occurs, uncheck the check box.

Field or Button	Description
Action: Send Trap	Check box indicating whether the MWTM should forward the event as a trap to other systems. If you: - Want MWTM to forward the event, check the check box. - Do not want MWTM to forward the event, uncheck the check box. This is the default setting.
Raise Alarm	 Caution This feature is for advanced users (Cisco developers and third-party integrators). If the Raise Alarm check box is checked, then, when this event happens, the MWTM raises an alarm that appears in the Active Alarms table.
Correlate	 Caution This feature is for advanced users (Cisco developers and third-party integrators). When you check this check box, you can then define a key in the Key field.
Key	 Caution This feature is for advanced users (Cisco developers and third-party integrators). You can define a key to correlate appropriate events. The EPM notification includes this key for use by the north-bound system. Right-click in the text field to select a key. You can also right-click in the field and choose Launch Text Editor, where you can update, clear, or discard your text changes.
Disable	Check box to disable this event without removing the event configuration from the <i>/opt/CSCOs/gm/etc</i> file.
Personalities	Clicking Edit opens the Personalities Editor, where you can select from the following networks by checking the box: - IPRAN - ITP - CSG1 - CSG2 - GGSN - BWG - HA Check the networks you want to include, then click Update, or click Discard to exit the window without saving your changes.

Field or Button	Description
Detect Flapping	Note This field is only active if you have defined a key. If you check the Detect Flapping check box, the following fields appear: - Flapping Threshold—Number of correlated events raised if the value matches or exceeds what is set for the Flapping Time Span in seconds value. - Flapping Time Span in seconds—At most, you can get one flapping event per flapping time span period. - Flapping Event Name—Name of flapping event. - Flapping Severity—Severity of flapping event. - Flapping Message—Detailed message for the flapping event.
Errors	Error messages associated with the event. Correct all errors before deploying the new event configuration.

Forwarding Events as Traps to Other Hosts

You use the MWTM to forward MWTM events to other hosts, in the form of SNMP traps. This operation enables the MWTM to integrate with high-level event- and alarm-monitoring systems such as the Cisco Info Center (CIC). These systems can provide a single high-level view of all alarm monitoring in your network, making it easier to detect and resolve problems.

To forward MWTM events to other hosts:

- Step 1** Specify the list of SNMP servers, or hosts, to which you want the MWTM to forward traps (see [Specifying a List of SNMP Servers for Trap Forwarding, page 9-40](#)).
- Step 2** Specify the events you want to forward, using one of these procedures. To forward:
 - a.** All MWTM events, click the **Send a trap for all events** radio button in the SNMP Servers Configuration window of the MWTM Event Editor. For more information, see [Specifying a List of SNMP Servers for Trap Forwarding, page 9-40](#).
 - b.** Only chosen events, edit the events in the MWTM Event Editor and check the **Send Trap** check box. For more information, see the description of the Send Trap field in [Configuring Trap, Status Alarm, or User Action Events, page 9-42](#).
- Step 3** (Optional) Specify new, more meaningful names for the events that you want to forward. If you do not specify a new message name for an event, the MWTM uses the default message name, MWTM. For more information, see the description of the Message Name field in [Configuring Trap, Status Alarm, or User Action Events, page 9-42](#).
- Step 4** Save your new event settings, deploy them to the MWTM server, and restart the MWTM server.



Note For more details, see the *Cisco Mobile Wireless Transport Manager 6.1 OSS Integration Guide*.

Setting Sounds for Events at an MWTM Client

You use the MWTM client interface to create and change event sound filters for the MWTM client. Event sound filters determine the sounds that the MWTM client plays when specific events are logged. The MWTM client plays the sounds even if the Event History window is not currently visible.

On Solaris and Linux systems, the root user can access the sound feature from a local or remote device. However, users other than the root user must use a local device and client, not a remote MWTM client accessed by using the xhost + UNIX command.

This section includes:

- [Listing Event Sound Filters, page 9-49](#)
- [Creating a New Event Sound Filter, page 9-50](#)
- [Adding a Sound File to the MWTM, page 9-52](#)
- [Changing an Existing Event Sound Filter, page 9-53](#)
- [Deleting an Event Sound Filter, page 9-53](#)
- [Playing and Muting Event Sounds, page 9-53](#)

Listing Event Sound Filters

You use the MWTM client interface to change the list of event sound filters that the MWTM client applies to events, or prevent the MWTM client from playing sounds for events.

To work with the list of event sound filters, choose **Tools > Event Sounds** from the MWTM main menu. The Event Sound Filters List dialog box appears.

The Event Sound Filters List dialog box lists all event sound filters that have been defined.

Field or Button	Description
Sound filters applied in order	Indicates the order in which sound filters are to be applied, from top to bottom. If an event matches two or more filters in the list, the top-most filter determines the sound that the MWTM client plays. This field is blank until you have created at least one new sound filter for events.
Move Up	Moves the chosen event sound filter up in the Sound filters applied in order list.
Move Down	Moves the chosen event sound filter down in the Sound filters applied in order list.
New	Opens the Event Sound Filters dialog box, which you use to create a new event sound filter.
Edit	Opens the Event Sound Filters dialog box, which you use to change an existing event sound filter in the Sound filters applied in order list.
Delete	Deletes the chosen event sound filter from the Sound filters applied in order list.
Mute Sounds	Check box indicating whether the MWTM client should play event sounds. To: • Play event sounds, check the check box. This is the default setting. • Not play event sounds, uncheck the check box.

Field or Button	Description
Client Disconnect Sound	Drop-down menu of sound files to choose from. When the connection to the MWTM server is lost, an error popup appears and the selected sound plays in a loop for as long as the MWTM client window remains open. Note After a server connection loss, you must set this sound again; otherwise, no sound will play the next time the server connection is lost.
Set Sound	Button to set the sound you chose for loss of server connection.
OK	Applies any changes you made to the event sound filters list and closes the Event Sound Filters List dialog box. When you are satisfied with the changes you made to the event sound filters list, click OK .
Apply	Applies any changes you made to the event sound filters list without closing the Event Sound Filters List dialog box.
Cancel	Closes the Event Sound Filters List dialog box without applying any changes to the event sound filters list.
Help	Shows online help for the current window.

Related Topics:

- [Setting Sounds for Events at an MWTM Client, page 9-49](#)
- [Managing Alarms and Events, page 9-1](#)

Creating a New Event Sound Filter

You use the MWTM client interface to create a new event sound filter. Open the Event Sound Filters List dialog box, as described in [Listing Event Sound Filters, page 9-49](#), then click **New**. The Event Sound Filters dialog box appears.

The Event Sound Filters dialog box contains:

Button or Field	Description
Filter Name	Name of the event sound filter file. Enter a name for the filter, then specify filter criteria for this event sound filter in the Event Sound Filter Criteria field.
Event Sound Filter Criteria	Table listing the filter criteria for this event sound filter. To add a criteria, select options from the drop-down list boxes: - To filter based on message text: a. Choose Message Text from the first drop-down list box. b. Choose Contains, Equals, Does Not Contain, or Does Not Equal from the second drop-down list box. c. Enter the message text in the character string field. - To filter based on event severity: a. Choose Severity from the first drop-down list box. b. Choose Equals or Does Not Equal from the second drop-down list box. c. Choose a severity, such as Normal, from the third drop-down list box, the message text.
Event Sound Filter Criteria (continued)	- To filter based on event category: a. Choose Category from the first drop-down list box. b. Choose Equals or Does Not Equal from the second drop-down list box. c. Choose a category, such as Status or Purge, from the third drop-down list box, the message text. - To filter based on the name of the node associated with the event: a. Choose Node from the first drop-down list box. b. Choose Equals or Does Not Equal from the second drop-down list box. c. Choose a node from the third drop-down list box. The MWTM lists all nodes that have been discovered in the drop-down list box.
More	Adds one or more additional filter criteria to the event sound filter. To add a filter criteria to the event sound filter, click More. The MWTM adds a new criteria to the bottom of the list.
Fewer	Removes one or more filter criteria from the event sound filter. To remove a filter criteria from the event sound filter, click Fewer. The MWTM deletes the last criteria in the list.

Button or Field	Description
Play this sound:	Drop-down list box indicating the sound to play if an event matches this event sound filter. The MWTM client sound files are stored in the MWTM client's <i>/sounds</i> directory. If you installed the MWTM client: - For Solaris/Linux in the default directory, <i>/opt</i>, then the sound file directory is <i>/opt/CSCOSgmClient/sounds</i>. - For Windows in the default directory, <i>/Program Files</i>, then the sound file directory is <i>C:\Program Files\MWTMClient\sounds</i>. To add a sound file to the MWTM, add it to the <i>/sounds</i> directory (see Adding a Sound File to the MWTM, page 9-52).
Play	Plays a sample of the sound chosen in the Play this sound drop-down list box.
OK	Applies any changes you made to the event sound filter criteria and closes the Event Sound Filters dialog box. When you are satisfied with the changes you made to the event sound filters, click OK.
Cancel	Closes the Event Sound Filters dialog box without applying any changes to the event sound filter criteria.
Help	Shows online help for the current window.

Related Topics:

- [Listing Event Sound Filters](#), page 9-49
- [Managing Alarms and Events](#), page 9-1

Adding a Sound File to the MWTM

You can add sound files to an MWTM client. The MWTM clients can play these sound file formats:

- AIFC
- AIFF
- AU
- SND
- WAV

**Note**

WAV files encoded using MPEG Layer-3 are not supported.

The MWTM client sound files are stored in the MWTM client's */sounds* directory. If you installed the MWTM client:

- For Solaris/Linux in the default directory, */opt*, then the sound file directory is */opt/CSCOSgmClient/sounds*.
- For Windows in the default directory, */Program Files*, then the sound file directory is *C:\Program Files\MWTMClient\sounds*.
- In a different directory, then the sound file directory is located in that directory.

**Note**

Sound files used by the MWTM web client must also be copied to the MWTM server sound directory at `/opt/CSCOs/gm/sounds`.

If for some reason the MWTM cannot play a specified sound file, the MWTM plays a default beep. For example, the MWTM cannot play a sound file if one of these conditions exists:

- The file has been moved or deleted from the `/sounds` directory.
- The `/sounds` directory has been deleted or cannot be found.
- Some other application is using all of the sound resources.
- No sound card is present.

Related Topics:

- [Creating a New Event Sound Filter, page 9-50](#)
- [Managing Alarms and Events, page 9-1](#)

Changing an Existing Event Sound Filter

You use the MWTM client interface to change an existing event sound filter. Open the Event Sound Filters List dialog box, as described in [Listing Event Sound Filters, page 9-49](#), select the filter in the **Sound filters applied in order** list, then click **Edit**. The MWTM shows the Event Sound Filters dialog box, populated with the chosen filter's settings.

Change the settings as needed, then click **OK**. The MWTM applies your changes and closes the Event Sound Filters dialog box.

Deleting an Event Sound Filter

You use the MWTM client interface to delete an existing event sound filter. Open the Event Sound Filters List dialog box, as described in [Listing Event Sound Filters, page 9-49](#), select the filter in the **Sound filters applied in order** list, then click **Delete**. The MWTM deletes the chosen filter.

Playing and Muting Event Sounds

You use the MWTM client interface to specify whether you want the MWTM client to play event sounds. To do so, open the Event Sound Filters List dialog box, as described in [Listing Event Sound Filters, page 9-49](#). To:

- Play event sounds, uncheck the **Mute Sounds** check box. This is the default setting.
- Not play event sounds, check the **Mute Sounds** check box.



CHAPTER 10

Viewing Network Topology



Note

The web interface does not support viewing the network topology. You can view the network topology only in the MWTM client interface.

In addition to tabular (text) views of your network, the Cisco Mobile Wireless Transport Manager (MWTM) provides a topological (graphical) view of the objects in your ITP or RAN-O network, including:

- Nodes
- RAN-O service modules
- Interfaces
- ITP signaling points
- ITP application servers
- ITP application server process associations
- ITP linksets
- Adjacent legacy nodes



Note

The MWTM does not manage legacy nodes (such as BSC, BTS, RNC, or Node B objects), but displays them in the topology map to help you visualize the interconnections between network objects.

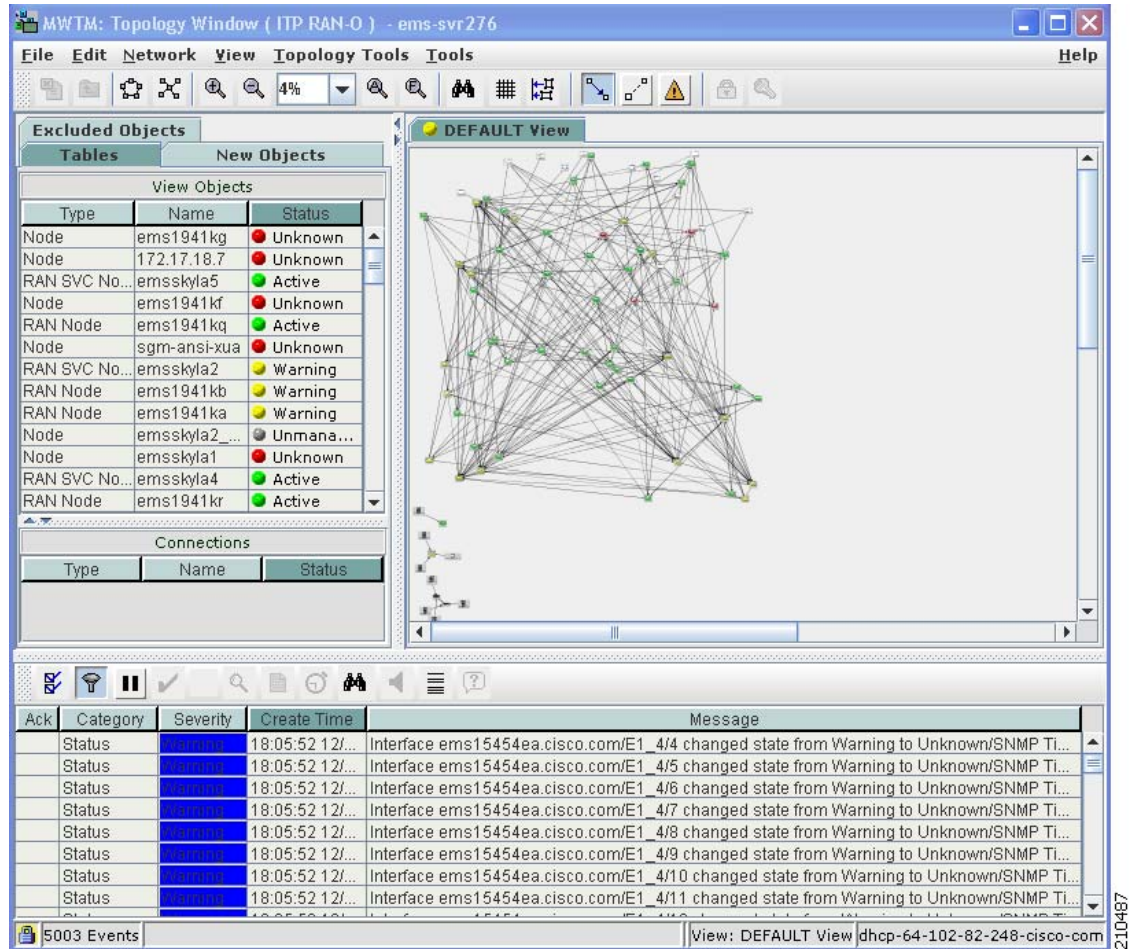
Any associated alarms also appear in the topology window. You can use the MWTM to customize the topological view (for details, see [Chapter 7, “Managing Views”](#)).

To view the topology of your network, use one of these procedures:

- Choose **View > Topology** from the MWTM main menu.
- Right-click an object, then choose **View > Center in Topo** in the right-click menu.

The topology window appears.

Figure 10-1 Topology Window



The topology window shows tabular information about MWTM objects in the left pane and the graphical topology map in the right pane. Alarms associated with the chosen object appear in the bottom pane.

The topology window contains:

- [Topology Menu, page 10-3](#)
- [Topology Toolbar Buttons, page 10-4](#)
- [Topology Tabs, page 10-6](#)
- [Topology Map, page 10-10](#)
- [Topology Alarm Pane, page 10-16](#)

The MWTM provides these functions related to the topology map:

- [Creating a Custom Layout, page 10-16](#)
- [Finding an Object, page 10-16](#)
- [Centering the Topology Map on an Object, page 10-17](#)
- [Displaying Detailed Information About a Topology Map Element, page 10-18](#)
- [Printing the Topology Map, page 10-18](#)
- [Saving the Topology Map as a JPEG File, page 10-18](#)
- [Selecting a Directory for the JPEG File, page 10-19](#)
- [Activating a Magnetic Grid on the Topology Map, page 10-20](#)
- [Specifying a Color for the Magnetic Grid, page 10-21](#)
- [Specifying a Background Color for the Topology Map, page 10-22](#)
- [Aligning Objects on the Topology Map, page 10-24](#)
- [Hiding and Displaying Non-ITP Nodes and Linksets, page 10-25](#)
- [Locking and Unlocking the Position of an Icon, page 10-25](#)
- [Improving Topology Performance, page 10-25](#)
- [Saving the Topology Map, page 10-26](#)
- [Restoring the Topology Map, page 10-27](#)

Related Topics:

- [Diagnosing a Typical Network Problem, page D-5](#)
- [Changing MWTM Server Poller Settings, page 3-2](#)
- [Chapter 7, “Managing Views”](#)

Topology Menu

The topology window is identical to the MWTM main menu. For detailed descriptions of the options it provides, see [Using the MWTM Main Menu, page 4-21](#).

Topology Toolbar Buttons

The topology window contains these toolbar buttons:

Button	Description
 Close view tab	Closes the currently visible view in the topology window. This option is dimmed if the currently visible view is the highest-level parent view.
 Open parent view	Opens the parent view of the currently visible view in the topology window. This option is dimmed if the currently visible view is the highest-level parent view.
 Lay out nodes in a circle	Shows the map in a circular layout.
 Lay out nodes in a spring	Shows the map in a spring layout. That is, the MWTM draws nodes with the most lines closer to the center of the map, and draws nodes with fewer lines farther away. This is the default setting the first time the map appears. Note You can change how far apart to space the nodes when the MWTM draws the spring layout (see Changing Topology Settings, page 5-14).
 Zoom in by a factor of 200%	Makes the map twice as large.
 Zoom out by a factor of 50%	Makes the map half as large.
 Zoom by percentage	Zooms the map by a chosen percentage. You can choose a percentage from the drop-down list box; or, enter a percentage and click Enter . Valid values are integers in the range 5 through 400.
 Zoom in on an area	Zooms in on the selected area of the map. Click the button, then click in the topology map and drag a rectangle around the area on which you want to zoom. The MWTM expands the selected area to fill the topology map.
 Zoom to fit window	Adjusts the size of the map to fit in the window. This is the default setting the first time the map appears.
 Find objects	Opens the Find Objects dialog box, which you use to find and highlight an object in the topology window.

Button	Description
 Set magnetic grid properties	Opens the Magnetic Grid Settings dialog box, which you use to activate and deactivate the magnetic topology grid, and modifies how it appears. With the grid activated, when you move objects on the topology map they automatically align with the grid.
 Align objects on map	Opens the Align Objects dialog box, which you use to align two or more objects on the topology map.
Hiding/Showing non-ITP nodes (ITP only) 	Hides or shows all non-ITP signaling points and linksets on the topology map. (Hidden signaling points and linksets still appear in the left pane.) The process determines whether the node's parent (visible on the topology maps) has an ITP MIB or not. If not, it is classified as a non-ITP node and it will be hidden or visible when the button is toggled. The MWTM automatically saves this setting (with non-ITP nodes and linksets either hidden or visible) with your preferences.
Node Dragging Optimizer 	Turns the Node Dragging Optimizer on or off: - When the Node Dragging Optimizer is On, the MWTM hides linkset lines as you drag an object around the topology map. The MWTM draws the linkset lines when you drop the object in its final position. This is the default setting. - When the Node Dragging Optimizer is Off, the MWTM continually redraws linkset lines as you drag an object around the topology map. The MWTM automatically saves this setting (with the Node Dragging Optimizer on or off) with your preferences.
Hiding/Showing Dangling Connections 	Hides or shows connections to objects that are not visible in the current view, which are called dangling connections. When the Hiding Dangling Connections is set to: Hide, the MWTM hides dangling connections. This is the default setting. Show, the MWTM shows dangling connections, drawing the objects in shades of gray to distinguish them from actual objects in the current view. The MWTM does not save this setting (with the Hiding Dangling Connections set to Show or Hide) when you save the view. To include a dangling connections in the current view, select the connection, then select Include In View.

Button	Description
 Show/Hide alarm pane	Shows or hides the alarm pane at bottom.
 Lock position or  Unlock position	Locks or unlocks the position of an icon on the topology map. Locking the position of an icon can be useful if you want to keep the icon in its position, and you want to ensure you do not move it inadvertently. Locked icons do not appear in the circular or spring layouts. To lock the position of an icon, select: - An unlocked icon, then select Lock position. - A locked icon, then select Unlock position. This is the default setting. The MWTM automatically saves this setting (with icon positions locked or unlocked) with your view.

Topology Tabs

In the topology window, you can access:

- [Tables Tab, page 10-6](#)
- [New Objects Tab, page 10-9](#)
- [Excluded Objects Tab, page 10-10](#)

Tables Tab

The Tables tab in the left pane of the topology window contains:

Name of Table	Description of Table Contents
View Objects	Shows information about the MWTM objects that are currently visible in the topology map.
Connections	Shows information about the connections associated with the object that you chose in the View Objects table, or the object currently chosen in the topology map.



Tip

If you cannot see the View Objects or Connections tables, click on the arrow bar  to expand.

- To redraw the topology map centered on a specific object, double-click the object in this table.
- You cannot select more than one object at a time in this table.
- To see the tooltip for each column in the table, place the cursor over a column heading.
- If a cell is too small to show all of its data, place the cursor over the cell to see the full data in a tooltip.

You can resize each column, or sort the table based on the information in one of the columns. By default, the MWTM sorts this table by Severity.

To:

- Display hidden columns, right-click in the table heading and check the check boxes for the columns you want to display.
- Hide columns, right-click in the table heading and uncheck the check boxes for the columns you want to hide.

For more information about resizing, sorting, displaying, or hiding columns, see [Navigating Table Columns, page 5-24](#).

The View Objects or Connections table contains:

Column	Description
Internal ID	Internal ID of the object. The internal ID is a unique ID for every object, that MWTM assigns for its own internal use. It can also be useful when the TAC is debugging problems. This column is hidden by default.
Type (View Objects)	Object types can be ITP only, RAN-O only, or General to all types of networks. General object types include: • Node—Any interconnecting node that is not an ITP node. • View—Custom view (if one exists). ITP only object types include: • ASP—An application server process. • SP—A signaling point. RAN-O only object types include: • CSR—Cell Site Router (CSR) node. • RAN SVC Node—A RAN service card in an Optical Networking System (ONS) node.
Type (Connections)	Connection types can be ITP only, RAN-O only, or General to all types of networks. ITP only object types include: • Linkset—A linkset associated with a signaling point. • ASPA—An application server process association associated with a signaling point. RAN-O only object types include: • RAN Backhaul—Virtual RAN backhaul associated with a RAN node or RAN SVC node. • GSM Interface—GSM interface associated with a RAN node or RAN SVC node. • Universal Mobile Telecommunications System (UMTS) Interface—UMTS interface associated with a RAN node or RAN SVC node.

Column	Description
Name	Name of the object.
Node	Name of the node associated with the object.
Notes	Indicates whether a note is associate with the object. This column is hidden by default.
Events	Indicates whether the object has a recent event. (Even if the server purges all of the events associated with the object, the MWTM continues to display the event icon  in this field.) During discovery, the MWTM might flag most objects with an event icon  . If the event icons are too distracting, choose Edit > Clear All Events from the MWTM main menu to remove them. This column is hidden by default.
Last Status Change	Date and time that the status of the object last changed. This column is hidden by default.
Severity	Severity of the alarm. Possible severities are:  Critical  Major  Minor  Warning  Informational  Indeterminate  Unmanaged  Normal You can customize this field (see Right-Click Menu for a Specific Alarm or Event, page 9-17).
Status	Current status of the object. Possible values are:  Active  Unknown  Unmanaged  Warning For detailed definitions of each status, see the “Status Definitions” section on page E-1 . This column is hidden by default.

Column	Description
Status Reason	Reason for the current status of the object. For a full list of possible reasons, see the <i>stateReasons.html</i> file. If you installed MWTM in: - The default directory, <i>/opt</i>, then the file resides at <i>/opt/CSCOsgm/apache/share/htdocs/eventHelp</i> directory. - A different directory, then the help directory and file reside in that directory. If the cell is too small to show all of the status reason, place the cursor over the cell to see the full status reason in a tooltip. The MWTM lists status reasons in order of decreasing magnitude. If two or more reasons apply, the reason of greatest magnitude appears. If the status reason is Unsupported Configuration, correct the configuration and enter the mwtm cleandiscover command to delete all current network data and begin a discovery of the network. If the status reason remains Unsupported Configuration, enter the mwtm clean command to restore the MWTM server to a state that would exist after a new installation of the MWTM, excluding the log files, which the MWTM retains. To also remove the log files, enter the mwtm cleanall command. For more information on the use of these commands, see Appendix B, “Command Reference.” This column is hidden by default.
Ignored	Indicates whether the object should be included when aggregating and displaying MWTM status information: - Uncheck the check box to include the object. This is the default setting. - Check the check box to exclude the object. Users with authentication level Power User (level 2) and higher can edit this field. This column is hidden by default.

New Objects Tab

The New Objects tab in the left pane of the topology window shows graphical elements for newly discovered objects, based on these criteria. If you are using an MWTM client with:

- The DEFAULT view set, this tab never contains any objects. In the DEFAULT view, the MWTM adds all newly discovered objects to the topology map as soon as they are discovered.
- A custom view set, this tab contains all objects discovered since the topology window was opened in this session that have *not* been excluded in the Excluded from View table of the View Editor window, or that are not in the current view.

To display the topology New Objects tab, select the New Objects tab in the left pane of the topology window.

To add a newly discovered object to the topology map, select one or more objects and hold down the left mouse button to drag them to the map.

To exclude a newly discovered object, use the View Editor window (see [Creating a New View, page 7-8](#)).

Excluded Objects Tab

The topology Excluded Objects tab in the left pane of the topology window shows graphical elements for excluded objects. Excluded objects are objects that you:

- Exclude from the topology map by right-clicking the object and selecting Exclude From View.
- Move to the Excluded from View table of the View Editor window (see [Creating a New View, page 7-8](#)).

To display the topology Excluded Objects tab, select the Excluded Objects tab in the left pane of the topology window.

To add an excluded object to the topology map, select the object hold down the left mouse button to drag it to the map. The MWTM no longer excludes the object, and removes it from the:

- Excluded Objects tab of the topology window.
- Excluded from View table of the View Editor window.

When you exclude a node from the topology map, the MWTM also removes adjacent legacy nodes from the map. When you add an excluded node back to the topology map, the adjacent legacy nodes reappear.

Topology Map

The topology map in the right pane of the topology window shows the objects and views in your network in an easy-to-read graphical format.

Views

If you have defined custom views, you can view them in the topology map. The MWTM shows a tab for each visible view. Each tab shows a colored ball that indicates the current status of that view:

-  Active
-  Warning



Note

For detailed definitions of each status, see [Status Definitions for Views, page E-2](#).

Excluded and Unmanaged Objects

The MWTM removes from the topology map any objects and their associated objects (including adjacent legacy nodes) that you exclude from the current view (see [Excluded Objects Tab, page 10-10](#), and [Creating a New View, page 7-8](#)).

If you unmanage an object from the topology map right-click menu (see [Topology Right-Click Menu: Object, page 10-15](#)) the MWTM marks the object status as Unmanaged and removes any adjacent legacy nodes from the topology map.

Tooltips

To see a tooltip, place the cursor over an object. For details on turning off tooltips, see [Changing Topology Settings, page 5-14](#).

Viewing Associated Objects

To view objects associated with a chosen object, in the:

- Tabs in the View Objects pane, click an object. Any associated objects (such as signaling points with associated linksets) appear in the Connections pane.
- Content area, click a single line, a heavy line , a diamond , circle , arrowhead , or double-triangle  to:
 - Highlight the closest associated node in the View Objects pane in a tab. For example, if a line connects node **sgm-2600a** and node **sgm-2600b**, and you click the line closer to node **sgm-2600a**, then the MWTM highlights that node in the View Objects pane.
 - Display all objects (if any) associated with that node in the Connections pane in a tab.
 - Highlight the clicked object (if it is configured) in the Connections pane in a tab.

Viewing Details for an Object

To display the Details tab for any object in the map, double-click it. If multiple options are possible, the Selection dialog box appears. Highlight the object, then click **Select**.

Navigating and Scrolling

To:

- Scroll around in the topology map using keyboard options, click anywhere in the map, then click the arrow, **Page Up**, and **Page Down** keys.
- Redraw the topology map centered on a specific object, double-click the object in the View Objects pane in a tab.
- Activate or change the magnetic topology grid, which can help you align objects when you move them, use the Magnetic Grid Settings dialog box (see [Activating a Magnetic Grid on the Topology Map, page 10-20](#)).
- Align two or more objects on the topology map, use the Align Objects dialog box (see [Aligning Objects on the Topology Map, page 10-24](#)).

Saving the Topology Map

To save the topology map as a JPEG file, use the Save as JPEG dialog box (see [Saving the Topology Map as a JPEG File, page 10-18](#)).

Hiding or Showing Dangling Connections

To hide objects that connect to objects that are not in the current view (called dangling connections), click the **Hiding/Showing Dangling Connections** button to set it to **Hide**. To show dangling connections, click the **Hiding/Showing Dangling Connections** button to set it to **Show**. The MWTM draws the objects in shades of gray to distinguish them from actual objects in the current view. The MWTM does not save this setting (with the Hiding Dangling Connections set to **Show** or **Hide**). To include a dangling object in the current view, right-click the object and select **Include In View**.

Locking and Unlocking Icon Positions

To lock the position of an icon on the topology map, select an unlocked icon, then select **Lock position**.

Locking the position of an icon can be useful if you want to keep the icon in its position, and you want to ensure that you do not move it inadvertently. The MWTM does not include locked icons in the circular or spring layouts.

To unlock the position of an icon on the topology map, click a locked icon, then select **Unlock position**.

Object Types in the Topology Map

The topology map might contain graphical elements for any of these objects, which the MWTM automatically assigns:



Note

Icon colors vary. The color of a graphical element indicates its current severity. If more than one object is configured on the connection, the color associated with the object that is in the most compromised state represents the severity color of the connection.

Object Type	Notes
 ASP	N/A
 BSC	Base Station Controller
 BTS	Base Transceiver Station
 Cisco 2600 series router	Cisco 2650, Cisco 2650XM, Cisco 2651, Cisco 2651XM
 Cisco 2811 series router	N/A
 Cisco 7202 series router	N/A
 Cisco 7204 series router	Cisco 7204, Cisco 7204VXR
 Cisco 7206 series router	Cisco 7206, Cisco 7206VXR
 Cisco 7301 series router	N/A
 Cisco 7304 series router	N/A
 Cisco 7505 series router	N/A

Object Type	Notes
 Cisco 7507 series router	Cisco 7507, Cisco 7507mx, Cisco 7507z
 Cisco 7513 series router	Cisco 7513, Cisco 7513mx, Cisco 7513z
 Cisco 7600 series router	Cisco 7603, Cisco 7603s, Cisco 7604, Cisco 7606, Cisco 7606s, Cisco 7609, Cisco 7609s, Cisco 7613
 Cisco MWR 1900 series router	N/A
 Cloud	A collection of objects, called a submap. A submap can also contain other submaps.
 IP device	Other than those listed previously (if assigned by a user; see Editing Properties, page 6-33)
 PGW	Cisco Public Switched Telephone Network (PSTN) Gateway (PGW) 2200 Softswitch
 Signaling point	An SCP, SSP, or STP, or an ITP instance (if the ITP is configured for multi-instance)

- A line indicates a single logical connection configured between two nodes. A line that:
 - Ends in a diamond  indicates that the connection has at least one configured interface or linkset associated with the node.
 - Ends in a circle  indicates that the connection is a virtual linkset, associated with a signaling point.
 - Does not end in a diamond  or circle  indicates that the interface or linkset is not configured on the node or cannot be shown because the MWTM is not managing the node.
 - Ends in an arrowhead  indicates that the connection is an application server process association.
 - Ends in a double-triangle  indicates a connection to a view that has multiple interfaces.
- A heavy line  indicates that two or more interfaces or linksets exist between two nodes, or between views and other objects.

In addition, users can assign graphical elements for these objects (see [Editing Properties, page 6-33](#)):

Object Type	Description
 Building	Icon representing a collection of objects in a building.
 City	Icon representing a collection of objects in a city.
 Database	Icon representing a database object.

Object Type	Description
 MatedPair	Mated pair of signaling points.
 MSC	Mobile switching center.
 Node-B	Radio transmission (or reception) unit for communication between radio cells in a UMTS network (Node-B resides at the cell site). Note The MWTM does not manage the Node B but displays the object in the topology window to help you visualize the network.
 RAN SVC Node	RAN service module card.
 RNC	Radio Network Controller used in a UMTS network to aggregate multiple Node-B units. Note The MWTM does not manage the RNC but displays the object in the topology window to help you visualize the network.
 SCP	Service control point.
 SSP	Service switching point.
 STP	Signal transfer point.
 Tower	Icon representing a PC tower.
 TrafficGenerator	Icon representing a device or emulator used to generate traffic, usually in a test environment.
 Unknown	Node that does not respond to SNMP requests for supported MIBs.
 Workstation	Icon representing a workstation.
 Workstation2	Icon representing a different workstation.

The topology map also provides right-click menus for elements. For more information, see these sections:

- [Topology Right-Click Menu: Map, page 10-15](#)
- [Topology Right-Click Menu: Object, page 10-15](#)

Topology Right-Click Menu: Map

The topology window provides a subset of the MWTM main menu as a right-click menu. To see this menu for a map, right-click in a blank area of the topology map. The topology map right-click menu displays:

Command	Description
Zoom In (Ctrl=)	Makes the map twice as large.
Zoom Out (Ctrl-- or Ctrl-Minus)	Makes the map half as large.
Zoom Area	Zooms in on the selected area of the map.
Zoom Fit	Adjusts the size of the map to fit in the window. This is the default setting the first time the map appears.
Layout > Circular	Shows the map in a circular layout.
Layout > Spring	Shows the map in a spring layout. That is, the MWTM draws nodes with the most links closer to the center of the map, and draws nodes with fewer links farther away. This is the default setting the first time the map appears.
Find	Opens the Find Objects dialog box, which you use to find and highlight an object in the topology window.
Restore Positions	Restores the view to the last saved view.
Save As JPEG (Ctrl-J)	Opens the Save as JPEG dialog box, enabling you to save the topology map to a JPEG file.
Magnetic Grid	Opens the Magnetic Grid Settings dialog box.
Change Background Color	Opens the Select Background Color dialog box, which you use to select a color for the background of the topology map.
Align	Opens the Align Objects dialog box, which you use to align two or more objects on the topology map.
Create Subview	Opens the View Editor window, which you use to select a new view to display in the topology window.
Open Parent View	Opens the parent view of the currently visible view in the topology window. This option is dimmed if the currently visible view is the highest level parent view.
Close View	Closes the currently visible view in the topology window. This option is dimmed if the currently visible view is the highest level parent view.

Topology Right-Click Menu: Object

The topology window displays a subset of the MWTM main menu as a right-click menu. To see this menu for any object in the topology window, right-click on an object in the topology map in the right pane. Options may vary depending on the chosen object type.

For a list of right-click menu options, see [Viewing the Right-Click Menu for an Object, page 8-3](#).

Topology Alarm Pane

The Alarm pane at the bottom of the topology window shows any current alarms on the chosen object. For details about the buttons and fields in the Alarm pane, see [Chapter 9, “Managing Alarms and Events.”](#)

Creating a Custom Layout

You can use the MWTM to create a custom layout for the topology map by manually moving objects on the map and by grouping them or isolating them to meet your needs. To move:

- A single object, click and drag the object to its new position.
- More than one object at the same time, press the Shift key and at the same time, select the objects and drag them. Objects keep their positions relative to one another.

When you are satisfied with the new topology map layout, choose **File > Save View** from the MWTM main menu. The MWTM saves the changes you have made to the network view, including any changes you have made to the topology map layout.

Finding an Object

Some topology maps are so large and complex that it can be difficult to find a specific object.

If the object appears in the tabs in the left pane, select the object, and the MWTM highlights it in the topology map.

If the object does *not* appear in the tabs in the left pane, click the **Find objects** button  in the topology window; or, choose **Edit > Find** from the MWTM main menu. The Find Object dialog box appears.

You can search by using the:

- Name
- Point code (for ITP signaling points)
- IP address (for RAN-O nodes)

The Find Object dialog box contains:

Field or Button	Description
Search string	Character string for which the MWTM should search.
OK	Launches the search. If: • No matching object is found, the MWTM shows an appropriate message. • Exactly one object is found that matches the Search string, the MWTM highlights the object in the Tables pane of the topology window, and zooms in on the chosen object in the topology map. • More than one object is found that matches the Search string, the Choose dialog box appears, in which you can select from a list of the found objects (see Using the Selection Dialog, page 10-17).
Cancel	Closes the Find Objects dialog box without launching the search.

Using the Selection Dialog

If more than one object matches the Search string in the Find Objects dialog box, the Selection dialog box appears.

The Selection dialog box contains:

Field or Button	Description
Select one in list	Type, Name, or Status of the found objects. Select the object you want to find.
Select	Highlights the chosen object in the left pane of the topology window, and zooms in on the chosen object in the topology map.
Cancel	Closes the Selection dialog box without selecting an object.

Centering the Topology Map on an Object

To redraw the topology map centered on a specific object, double-click the object in one of the tabs.

Displaying Detailed Information About a Topology Map Element

To display detailed information about an element in the map, double-click it in the map, then respond to the prompts. Double click:

- An object to view the Details tab in the MWTM main menu for that object.
- A single line, or a diamond , circle , or arrowhead  at the end of a single line, to display the MWTM main window details for that linkset or application server process association.
- A double-triangle  at the end of a heavy line  to display the Selection dialog box. (A heavy line indicates that two or more interfaces or linksets exist between two objects, or between views and other objects.) Then, select one of the interfaces or linksets to display the Selection dialog box for that interface or linkset.

Printing the Topology Map

To print the topology map, see [Printing Windows, page 5-25](#).

Saving the Topology Map as a JPEG File

You can use the MWTM to save the topology map to a JPEG file. You can save the entire topology map, or just the current window.

To save the topology map to a JPEG file, choose **Topology Tools > Save as JPEG** from the topology window.

The Save as JPEG dialog box appears. The Save as JPEG dialog box contains:

Field or Button	Description
All	Saves the entire topology map as a JPEG file. This check box is checked by default.
Current Window	Saves just the portion of the topology map visible in the current window as a JPEG file. This check box is unchecked by default, which saves the entire map; not just the current window.
Quality	Specifies the quality of the JPEG file, from 0 (lowest quality) to 1.0 (highest quality). The default setting is 0.7, which is sufficient for most JPEG files.
Max. Size	Specifies the size of the JPEG file, in pixels. Choose a value from the drop-down list box. The valid range is 400-2400 pixels. The default value is 400 pixels, which is sufficient for most JPEG files.

Field or Button	Description
Name	Enter a name for the JPEG file, or accept the default filename, <i>out.jpg</i>. The default directory for the JPEG file is the directory in which you installed the MWTM client: - In Solaris/Linux, the default installation directory for the MWTM client is <i>/opt/CSCOsgmClient</i>. - In Windows, the default installation directory for the MWTM client is <i>C:\Program Files\SGMClient\</i>. - If you installed the MWTM client in a different directory, then the installation directory resides in that directory. If you do not want to save the JPEG file to the default directory, click Browse to select a different directory.
Browse	Opens the Save dialog box for a topology map, which you use to specify or select a name when you save the JPEG file. If you do not want to save the JPEG file to the default directory, click Browse to select a different directory.
Save	Saves the JPEG file and closes the Save as JPEG dialog box.
Cancel	Closes the Save as JPEG dialog box without saving the JPEG file.

Selecting a Directory for the JPEG File

You can use the MWTM to specify or select a name or directory when you save a topology map to a JPEG file. You can save the entire topology map, or just the current window.

To specify a name or directory for the JPEG file, click **Browse** in the Save as JPEG dialog box.

The Save dialog box appears for a topology map. The Save dialog box for a topology map contains:

Field or Button	Description
Save In	Selects the directory in which you want to save the topology map JPEG file. You can accept the default directory, or select a new directory from the drop-down list box.
File Name	Enter a name for the JPEG file, or select a file from those listed in the Save In field.
Files of Type	Specifies the type of file to save, and shows all files of that type in the chosen directory. Choose a file type from the drop-down list box: All files—Shows all files in the chosen directory, and saves the topology map file as a JPEG file. jpg files—Shows only JPEG files in the chosen directory, and saves the topology map file as a JPEG file. This is the default value.
 Up One Level	Shows the subfolders and files that are in the folder that is up one level from the currently visible folder.
 Desktop	Shows the subfolders and files that are on your workstation desktop.

Field or Button	Description
 Create New Folder	Creates a new subfolder in the currently visible folder.
 List	Shows only icons for subfolders and files.
 Details	Shows detailed information for subfolders and files, including their size, type, date they were last modified, and so on.
Save	Saves the file and closes the Save dialog box for a topology map. When you are satisfied with the settings, click Save . The MWTM closes the Save dialog box for a topology map and populates the Name field in the Save as JPEG dialog box with the new name and directory.
Cancel	Closes the Save dialog box for a topology map without saving the file.

Activating a Magnetic Grid on the Topology Map

You can use the MWTM to activate the magnetic topology grid and change how it appears. With the grid activated, when you move objects on the topology map they align with the grid.



Note

Magnetic grid settings are *not* saved when you save the view.

To activate or change the magnetic topology grid, choose **Topology Tools > Magnetic Grid** from the topology window. The Magnetic Grid Settings dialog box appears. The Magnetic Grid Settings dialog box contains:

Field or Button	Description
Grid Activated	Specifies whether the magnetic topology grid is activated. To: • Activate the grid, check this check box. • Deactivate the grid, uncheck this check box. This is the default setting.
Display Grid	Specifies whether the grid should be visible on the topology map. To: • Display the grid, check this check box. This is the default setting. • Hide the grid, uncheck this check box. If Grid Activated is not checked, this check box is dimmed.
Grid Spacing	Specifies the spacing between lines on the grid, in pixels. To specify the spacing between lines on the grid, in pixels, check the Grid Activated check box, then select a Grid Spacing level. The valid range is 0-150 pixels. The default setting is 50 pixels, which is sufficient for most topology maps.

Field or Button	Description
Grid Color	Opens the Select Grid Color dialog box. To specify a color for the grid, check the Grid Activated check box, then click Change Color in the Grid Color field. The MWTM opens the Select Grid Color dialog box.
OK	Sets the new grid settings and closes the Magnetic Grid Settings dialog box. When you are satisfied with the magnetic grid settings, click OK .
Cancel	Closes the Magnetic Grid Settings dialog box without changing any settings.

Specifying a Color for the Magnetic Grid

You can use the MWTM to customize the color of the magnetic topology grid.



Note

The grid color is *not* saved when you save the view.

To specify a color for the grid, check the Grid Activated check box in the Magnetic Grid Settings dialog box, then click **Select** in the Grid Color field.

The Select Grid Color dialog box opens. The Select Grid Color dialog box contains:

- [Swatches Pane \(Recommended\), page 10-21](#)
- [HSB Pane, page 10-21](#)
- [RGB Pane, page 10-22](#)
- [Select Grid Color Field and Buttons, page 10-22](#)

Related Topic:

[Activating a Magnetic Grid on the Topology Map, page 10-20.](#)

Swatches Pane (Recommended)

You can use the Swatches pane of the Select Grid Color dialog box to select a grid color from a set of color swatches. This is the recommended method for selecting a grid color.

To display the Swatches pane, click the Swatches tab in the Select Grid Color dialog box.

To select a grid color, select a swatch. The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

HSB Pane

You can use the HSB pane of the Select Grid Color dialog box to select a grid color based on color hue, saturation, and brightness (HSB).

To display the HSB pane, click the HSB tab in the Select Grid Color dialog box.

To select a grid color, use one of these procedures:

- Select a color range on the vertical color bar, then select a specific color by moving the cursor around on the color square.
- Enter specific values in the hue (H), saturation (S), and brightness (B) fields.

The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

RGB Pane

You can use the RGB pane of the Select Grid Color dialog box to select a grid color based on the red, green, and blue (RGB) content of the color.

To display the RGB pane, click the RGB tab in the Select Grid Color dialog box.

To select a grid color, select values for the Red, Green, and Blue fields. The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

Select Grid Color Field and Buttons

The Select Grid Color dialog box contains:

Field	Description
Preview	Shows a preview of the currently chosen grid color. Whichever method you choose to select a grid color, the chosen color appears in the Preview field. When you are satisfied with the color, click OK .
OK	Sets the grid color as shown in the Preview field, and closes the Select Grid Color dialog box.
Cancel	Closes the Select Grid Color dialog box without selecting a grid color.
Reset	Resets the grid color to its initial setting.

Specifying a Background Color for the Topology Map

You can use the MWTM to customize the background color of the topology map.



Note

The background color is *not* saved when you save the view.

To specify a background color for the topology map, right-click in a blank area of the topology map, then select **Change Background Color** from the right-click menu.

The Select Background Color dialog box contains:

- [Swatches Pane \(Recommended\), page 10-23](#)
- [HSB Pane, page 10-23](#)
- [RGB Pane, page 10-23](#)
- [Select Background Color Field and Buttons, page 10-23](#)

Swatches Pane (Recommended)

You can use the Swatches pane of the Select Background Color dialog box to select a background color from a set of color swatches. This is the recommended method for selecting a background color.

To display the Swatches pane, click the Swatches tab in the Select Background Color dialog box.

To select a background color, select a swatch. The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

HSB Pane

You can use the HSB pane of the Select Background Color dialog box to select a background color based on color hue, saturation, and brightness (HSB).

To display the HSB pane, click the HSB tab in the Select Background Color dialog box.

To select a grid color, use one of these procedures:

- Select a color range on the vertical color bar, then select a specific color by moving the cursor around on the color square.
- Enter specific values in the hue (H), saturation (S), and brightness (B) fields.

The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

RGB Pane

You can use the RGB pane of the Select Background Color dialog box to select a background color based on the red, green, and blue (RGB) content of the color.

To display the RGB pane, click the RGB tab in the Select Background Color dialog box.

To select a background color, select values for the Red, Green, and Blue fields. The chosen color appears in the Preview field. When you are satisfied with the color, click **OK**.

Select Background Color Field and Buttons

The Select Background Color dialog box contains:

Field	Description
Preview	Shows a preview of the currently chosen background color. Whichever method you choose to select a background color, the chosen color appears in the Preview field. When you are satisfied with the color, click OK .
OK	Sets the background color as shown in the Preview field, and closes the Select Background Color dialog box.
Cancel	Closes the Select Background Color dialog box without selecting a background color.
Reset	Resets the background color to its initial setting.

Aligning Objects on the Topology Map

**Note**

To unalign objects, drag and drop the object to move it on the topology map.

You can use the MWTM to align two or more objects on the topology map. You can align the objects based on their left, right, top, or bottom edges, or you can center them in the map. The MWTM saves the alignment when you save the view.

To align objects, choose the objects that you want to align, then choose **Topology Tools > Align** from the topology window. The Align dialog box appears. The Align dialog box contains:

Field	Description
Vertically: None	Does not align the chosen objects vertically.
Vertically: Left	Aligns the chosen objects vertically, aligned with the left edge of the left chosen object.
Vertically: Center	Aligns the chosen objects vertically, with centers aligned.
Vertically: Right	Aligns the chosen objects vertically, aligned with the right edge of the right chosen object.
Vertically: Side by side	Aligns the chosen objects vertically, aligned side-by-side, with no horizontal space between the objects. (There might still be vertical space between the objects.)
Horizontally: None	Does not align the chosen objects horizontally.
Horizontally: Top	Aligns the chosen objects horizontally, aligned with the top edge of the top chosen object.
Horizontally: Center	Aligns the chosen objects horizontally, with centers aligned.
Horizontally: Bottom	Aligns the chosen objects horizontally, aligned with the bottom edge of the bottom chosen object.
Horizontally: Side by side	Aligns the chosen objects horizontally, aligned side-by-side, with no vertical space between the objects. (There might still be horizontal space between the objects.)
Apply	Aligns the chosen objects and keeps the Align dialog box open, enabling you to continue aligning objects.
OK	Aligns the chosen objects and closes the Align dialog box.
Cancel	Closes the Align dialog box. Changes you applied are saved; other changes are not saved.
Help	Opens the Help window for this object.

Hiding and Displaying Non-ITP Nodes and Linksets

**Note**

This function applies only to ITP objects. If you have not discovered ITP objects in your network, the Hiding/Showing Non-ITP Nodes button does not appear.

To hide all non-ITP nodes and linksets on the topology map (the default setting), click the **Hiding/Showing Non-ITP Devices** button. (The hidden signaling points and linksets are still visible in the left pane.)

To display all hidden nodes and linksets on the topology map, click the **Hiding/Showing Non-ITP Devices** button again.

The MWTM automatically saves this setting (with non-ITP nodes and linksets either hidden or visible) with your preferences.

Locking and Unlocking the Position of an Icon

You can use the MWTM to lock the position of an icon on the topology map. Locking the position of an icon can be useful if you want to keep the icon in its position, and you want to ensure that you do not move it inadvertently. The MWTM does not include locked icons in the circular or spring layouts.

- To lock the position of an icon on the topology map, right-click an unlocked icon, then select **Lock Position**.
- To unlock the position of an icon on the topology map, right-click a locked icon, then select **Unlock Position**. This is the default setting.

The MWTM saves this setting (with icon positions locked or unlocked) when you save the view.

Improving Topology Performance

In certain cases, you can enhance topology performance by:

- [Turning Off Antialiasing, page 10-25](#)
- [Connecting Locally for Large Networks—Solaris Clients Only, page 10-26](#)
- [Hiding and Redrawing Connections When Redrawing, page 10-26](#)
- [Hiding and Showing Connections When Redrawing, page 10-26](#)

Turning Off Antialiasing

Antialiasing, which is on by default, improves the appearance of the icons and connections in the topology map. However, antialiasing can cause an unexpected delay in the MWTM client on a remote workstation (that is, a Solaris/Linux workstation using xhost, or a Windows workstation by using an X-Window system emulator such as eXceed or Reflection X).

You can use the MWTM to turn off antialiasing to improve the performance of the MWTM client on a remote workstation. To do so, check the **X Performance Enhancer (AntiAliasing Off)** check box in the Topology settings in the Preferences window (see [Changing Topology Settings, page 5-14](#)).

To turn antialiasing back on, uncheck the check box.

**Tip**

Keep in mind that for small networks, performance is always better if you access the MWTM by installing the MWTM client on the remote workstation.

Connecting Locally for Large Networks—Solaris Clients Only

If you are using a remote Solaris client and you have a large network, use a local Solaris client with a graphics card and an attached monitor, rather than remote access, to improve topology performance.

**Note**

This issue might also cause an unexpected delay in the unsupported Linux client.

Hiding and Redrawing Connections When Redrawing

To aid performance, you can use the MWTM to hide connection lines as you drag an object around the topology map, then re-draw the connection lines when you drop the object in its final position. To do so, click the **Node Dragging Optimizer** button to turn it on. This is the default setting.

To have the MWTM continually redraw connection lines as you drag an object around the topology map, click the **Node Dragging Optimizer** button to turn it off.

The MWTM automatically saves this setting (with the Node Dragging Optimizer on or off) with your preferences.

Hiding and Showing Connections When Redrawing

To aid performance, you can use the MWTM to hide connections linked to objects that are not in the current view, called dangling connections. To do so, click the **Hiding/Showing Dangling Connections** button to set it to Hide. This is the default setting.

To show dangling connections, click the **Hiding/Showing Dangling Connections** button to set it to Show. The MWTM draws the connections in shades of gray to distinguish them from actual objects in the current view.

The MWTM does *not* save this setting (with the Hiding Dangling Connections set to Show or Hide) when you save the view.

To include a dangling connection in the current view, right-click the connection and select **Include In View**.

Saving the Topology Map

When you are ready to close the topology window, choose **File > Save View** from the MWTM main menu. The MWTM prompts you to save any changes you made to the network view, including any changes you have made to the topology map layout, and closes the window (see [Closing the View Editor Window](#), page 7-14).

Restoring the Topology Map

You can use the MWTM to restore the topology map to the way it looked in the last saved view. To do so, choose **Topology Tools > Restore Positions** from the topology window. The MWTM restores the view.



CHAPTER 11dc

Accessing Data from the Web Interface

This chapter provides information about accessing Cisco Mobile Wireless Transport Manager (MWTM) data from the MWTM web interface by using a web browser. This chapter includes:

- [Accessing the MWTM Web Interface, page 11-1](#)
- [Overview of the MWTM Web Interface, page 11-2](#)
- [Displaying the Home Page, page 11-8](#)
- [Displaying the Administrative Page, page 11-12](#)
- [Displaying Alarms and Events, page 11-30](#)
- [Displaying Summary Lists, page 11-31](#)
- [Displaying Reports, page 11-33](#)
- [Displaying Objects in a View, page 11-33](#)
- [Displaying RAN-O Historical Statistics, page 11-33](#)
- [Displaying CSG2 Real-Time Statistics, page 11-44](#)
- [Displaying BWG Real-Time Statistics, page 11-49](#)
- [Displaying HA Real-Time Statistics, page 11-62](#)
- [Displaying GGSN Real-Time Statistics, page 11-65](#)
- [Displaying PWE3 Real-Time Statistics, page 11-72](#)
- [Displaying TDM Real-Time Statistics, page 11-72](#)

Accessing the MWTM Web Interface

The home page of the MWTM web interface is the first window to appear when you launch the MWTM web interface.

To access the MWTM web interface, use one of these methods:

- Open a browser and enter **`http://mwtm_server:1774`** in the Address field. (1774 is the default port.)



Note Accessing the MWTM web interface through a URL other than **`http://mwtm_server:1774`** is not supported.

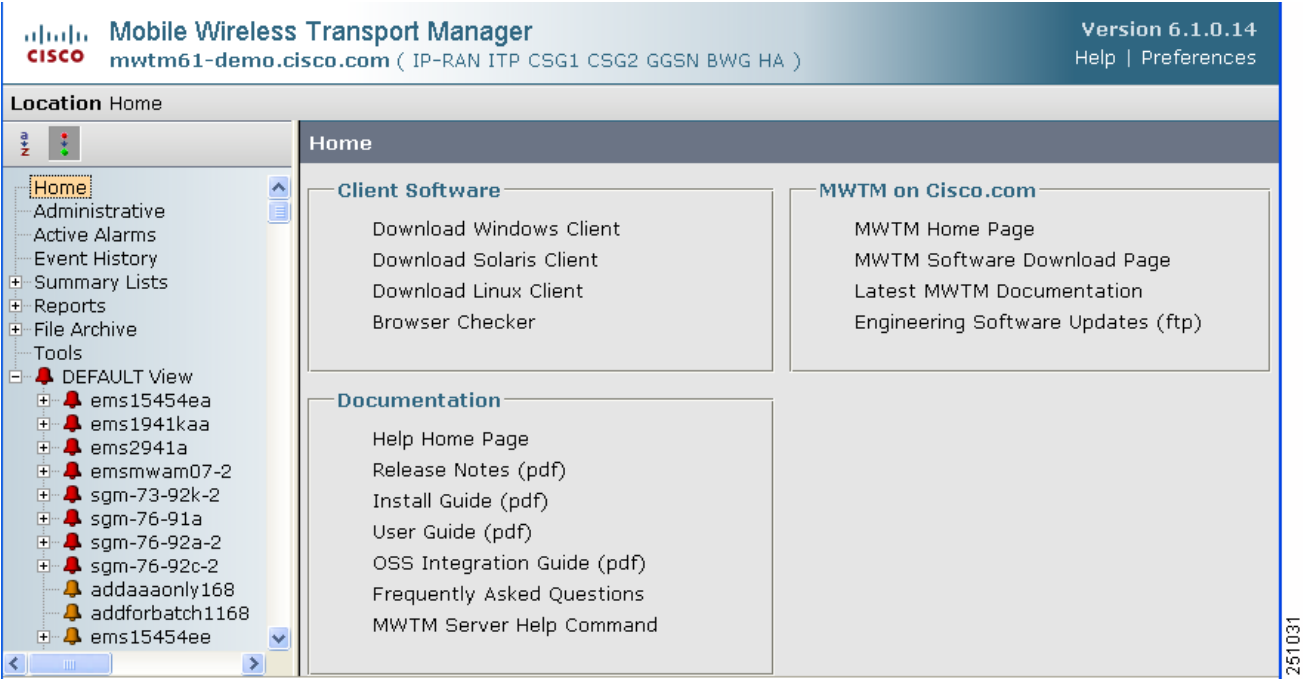
- From the MWTM client interface, choose **View > Web > Home**.

The MWTM Home page window opens in the browser window. For details about the Home page, see [Displaying the Home Page, page 11-8](#).

Overview of the MWTM Web Interface

The MWTM web interface shows basic information about the events and objects that the MWTM manages.

Figure 11-1 MWTM Web Interface



The MWTM web interface shows:

Pane	Description
Title Bar	Shows: - Mobile Wireless Transport Manager, version, and server name - Managed networks (can be any combination of IPRAN, ITP, CSG1, CSG2, GGSN, BWG and/or HA) - Logout (appears only if you enable user access; see Configuring User Access, page 2-1) - Help—Click this link to access context-sensitive online help - Preferences—Click this link to access preferences that you can change from the web interface (see Changing Web Preference Settings, page 5-20)
Location bar	Shows where you currently are in the MWTM navigation tree.

Pane	Description
Navigation Tree	In the left pane, shows a tree of information organized by categories (see MWTM Web Interface Navigation Tree, page 11-3).
Content Area	In the right pane, shows detailed information about the object chosen in the navigation tree (see MWTM Web Interface Content Area, page 11-4).

MWTM Web Interface Navigation Tree

You can easily navigate the features of the MWTM web interface by using the navigation tree in the left pane. By default, the navigation tree is sorted by alarm severity, with objects having the most severe alarms appearing at the top of the tree.



Note

To learn more about alarm severity, see [Chapter 9, “Managing Alarms and Events.”](#)

To view detailed information about a selection in the navigation tree, click the item in the tree. The content area in the right pane shows details about the chosen item. A plus (+) or minus (-) just to the left of the item indicates whether the item has subtending items under its domain.

The MWTM automatically updates the navigation tree when changes occur to discovered nodes or to the network. When any changes occur in the MWTM client navigation tree, the MWTM web interface reflects these changes in its navigation tree. For example, if you delete a node in the MWTM client, the MWTM web interface removes that node from its navigation tree.



Note

For information about the navigation tree in the MWTM client interface, see [MWTM Client Navigation Tree, page 4-19](#).

The MWTM web interface navigation tree contains:

GUI Element	Description
 Sort tree by name	Sorts all content in the navigation tree alphabetically by name.
 Sort tree by status	Sorts all content in the navigation tree by status, from the highest alarms to the lowest.
Home	Shows links to MWTM client software, Cisco documentation, and information about the MWTM on the Cisco web (see Displaying the Home Page, page 11-8).

GUI Element	Description
Administrative	Shows MWTM system information including messages, logs, status, and properties (see Displaying the Administrative Page, page 11-12). If MWTM User-Based Access is enabled, only users with authentication level 3 (Network Operator) and higher can see all options. Users of all other levels see only the System Information and System Status panes.
Active Alarms	Shows alarms (see Displaying Alarms and Events, page 11-30).
Event History	Shows information about the events delivered by the MWTM event logger and event processor for events that the MWTM event logger and event processor deliver for all objects in the current network view (see Displaying Alarms and Events, page 11-30).
Summary Lists	Shows summaries of all objects that the MWTM manages (see Displaying Summary Lists, page 11-31).
Reports	For ITP and RAN-O networks: - Shows Event reports for RAN-O and ITP networks (see Setting an Alarm or Event Filter, page 9-18). For ITP networks only: - Shows ITP historical reports for a specified time period (see Displaying Reports, page 11-33). For RAN-O networks only: - Shows RAN-O shorthaul and backhaul performance and error reports (see Viewing RAN Reports, page 12-75). If MWTM User-Based Access is enabled, only users with authentication level 4 (Network Administrator) and higher can see the Reports menu.
File Archive	Shows file archives (events and ITP reports). See Viewing Reports, page 12-6 .
Tools	Provides tools for launching CiscoWorks, CiscoView, Device Center, CSG Service Manager, and GGSN Service Manager (if integrated with MWTM). Also provides a search tool for Home Agent (HA) subscribers (see Tools, page 11-31).
DEFAULT View	Shows a current list of nodes in the DEFAULT view (see Displaying Objects in a View, page 11-33).

MWTM Web Interface Content Area

The content area of the MWTM client interface is fully described in [MWTM Client Content Area, page 4-19](#). That description also applies to the web interface. Additional navigational features that appear only in the web interface include:

- [Customizing the Date Range, page 11-5](#)
- [Using the Toolbar, page 11-5](#)

Customizing the Date Range

Some windows require that you select date ranges for generating historical graphs (see [Displaying RAN-O Historical Statistics, page 11-33](#)). Standard date ranges (for example, Last 24 Hours or Last 7 Days) are available from a drop-down menu. However, if you want to customize the date range:

Step 1 Click the **Customize Date and Time Range** tool  in the toolbar of the content area. A dialog box appears.

Step 2 Enter a:

- a. Begin Date and End Date; or, select those dates by clicking the Calendar tool .
- b. Begin Hour and End Hour from the drop-down menus, if they are available.



Note The dialog box shows an error if the End Date is equal to or less than the Begin Date. Correct the error before proceeding.

Step 3 Click **OK** to accept the date and time changes; or, **Cancel** to cancel this operation.

The MWTM web interface generates a report for the specified time period.

Using the Toolbar

Depending upon the object you select in the navigation tree, the web interface toolbar provides these tools and options:

Tool or Function	Description
Last Updated	Date and time the MWTM last updated the information on the page.
Page	Shows where you are (page X of X total pages) and lists the total number of entries.
 Refresh	Forces a refresh of the current web page. Click this icon to refresh the current page.
Status Refresh Interval	Allows you change the default refresh interval of 180 seconds. Enter a value between 180 and 900 seconds. Note Changes you make are temporary to the current page. Navigating away from the page sets the status refresh interval back to the default setting. To change the default setting, see Changing Web Preference Settings, page 5-20 .

Tool or Function	Description
Page Size	Drop-down list of different page sizes (the number of table rows in the display). Click the drop-down arrow to select a different value. The value that you select becomes the default page size for all pages in the web interface.  Caution Setting the Page Size to Unlimited may cause your browser to stop responding if the number of table rows is large. The title bar displays the current page and total number of table entries.
>	Advances the display to the next page of information.
>>	Advances the display to the last page of information.
<	Advances the display to the previous page of information.
<<	Advances the display to the first page of information.
 Modify event filter	Opens the Event Filter dialog box. You can create a filter to display only the events in which you are interested (see Setting an Alarm or Event Filter, page 9-18).
 Remove filter	Applies or removes a filter that you created.
Archived	Link that shows only archived alarms or events. This link appears when you select Event History or Active Alarms in the navigation tree. It also appears when you click the Alarms tab or Recent Events tab for a specific object.  Caution In the <i>Server.properties</i> file, you can limit the number of rows in the archived events table with the MAX_ARCHIVED_EVENT_DB_ROWS property. The default value is 200,000. Increasing this value can have severe impact on server performance and can cause the server to run out of memory.
 Customize Date and Time Range	Opens the Customize Date and Time Range dialog box (see Customizing the Date Range, page 11-5).
 Graph Series Editor	Opens the Graph Series Editor dialog box, which provides a check box for each shorthaul that is associated with the chosen RAN backhaul. To display a data series, check the check box. To hide a series, uncheck the check box. If you uncheck all shorthauls and click OK, the graph shows the default series of shorthauls. The MWTM displays no more than 12 series by default. To change this default setting, see Display Series Dialog Box, page 8-113.
 Run	Runs the report type for the chosen duration.
 Export	Exports the raw graph data to a report with comma-separated values (CSV file). You can save this file to disk or open it with an application that you choose (for example, Microsoft Excel).

Tool or Function	Description
Data Range	Label that shows the chosen time range for the historical statistics.
Type	Drop-down list of report types.
Duration	Drop-down list of default time ranges. Select one of these options, then click the Run tool  . To specify a nondefault time range, click the Customize Date and Time Range tool  .
Output Type	Drop-down menu that provides these options: - Graph—Displays statistical data in graphs and tables - Table—Presents statistical data in tabular format only - CSV—Exports statistical data using comma-separated values
 Pause	Pauses the page refresh feature. Click Pause to disable the page refresh that would normally occur after the Status Refresh Interval. Click Pause again to re-enable the Status Refresh Interval.
 Edit Notes	Enables you to edit or add notes for events.
Slow Poller Interval	Allows you to change the default slow poller interval of 60 seconds. Enter a value between 60 and 300 seconds. Note Changes you make are temporary to the current page. Navigating away from the page sets the status refresh interval back to the default setting. To change the default setting, see Changing Web Preference Settings, page 5-20 .
Fast Poller Interval	Allows you to change the default fast poller interval of 15 seconds. Enter a value between 5 and 60 seconds. Note Changes you make are temporary to the current page. Navigating away from the page sets the status refresh interval back to the default setting. To change the default setting, see Changing Web Preference Settings, page 5-20 .
Reset Counters	Enables you to modify the counter reset settings to one of the following: - Show counters since reboot - Show counters since last poll - Show counters since user reset
Launch	Drop-down list of applications you can launch: - CiscoView - Device Center After you choose the application, click the  Run icon to launch it.
Severity	Drop-down list of the severities of alarms or events. Severity can be Critical, Major, Minor, Warning, Informational, Indeterminate, or Normal. This drop-down list appears when you select Event History or Active Alarms in the navigation tree. It also appears when you click the Alarms tab or Recent Events tab for a specific object.

Tool or Function	Description
Change Severity	Button to change the severity level of an alarm or event. To change the severity level, select one or more alarms or events by clicking the corresponding check boxes, choose a severity from the Severity drop-down list, then click Change Severity. This button appears when you select Event History or Active Alarms in the navigation tree. It also appears when you click the Alarms tab or Recent Events tab for a specific object.
Clear Selection	Link to clear the selection of one or more events or alarms. To select one or more alarms or events, check the corresponding check boxes. To clear the selection, click the Clear Selection link. This button appears when you select Event History or Active Alarms in the navigation tree. It also appears when you click the Alarms tab or Recent Events tab for a specific object.
Toolbar for alarms and events	The web interface provides the same toolbar for alarms and events as the client interface. For full descriptions of these tools, see Toolbar Buttons, page 9-14 .

Displaying the Home Page

The MWTM web interface Home page provides access to MWTM client software, Cisco documentation, and information about the MWTM.

To access the Home page of the MWTM web interface, click **Home** under the navigation tree in the left pane.

The content area in the right pane shows these GUI elements:

Pane	GUI Element	Description
Client Software	Download Windows Client	Shows the download instructions for the: - Windows client - Solaris client - Linux client
	Download Solaris Client	
	Download Linux Client	
	Browser Checker	For details, see Downloading the MWTM Client from the Web, page 11-9 .

Pane	GUI Element	Description
MWTM on Cisco.com	MWTM Home Page Engineering Software Updates (FTP) MWTM Software Download Page Latest MWTM Documentation	Shows hyperlinks to: • MWTM information on the Cisco web • Software updates provided by Cisco Engineering • MWTM software download from Cisco.com • Most recent versions of MWTM documentation For details, see Accessing Software Updates and Additional Information, page 11-11 .
Documentation	Help Home Page User Guide Install Guide Release Notes Frequently Asked Questions MWTM Server Help Command	Shows: • Online Help system for the MWTM • PDF versions¹ of the: – <i>User Guide for the Cisco Mobile Wireless Transport Manager</i> – <i>Installation Guide for the Cisco Mobile Wireless Transport Manager</i> – <i>Release Notes for the Cisco Mobile Wireless Transport Manager</i> • HTML version¹ of the FAQs • CLI output of the mwtm help command For details, see Viewing the MWTM Technical Documentation, page 11-12 .

1. To access the latest versions, go to the parent index for Cisco MWTM user documents:
http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html

Downloading the MWTM Client from the Web

You can access the MWTM client installation software for Linux (unsupported), Solaris, and Windows from the MWTM web interface Home page. This access is useful if you do not have the CD-ROM, or if you prefer to download the software by using your web browser. Once you have downloaded the MWTM client installation software to your workstation, you must install the software on your local system.

For more information about installing the MWTM client software by using a web server, see the following chapters in the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*:

- “Installing the MWTM on Solaris”
- “Installing the MWTM on Windows”
- “Installing the MWTM on Linux”

Downloading the Solaris Client

To access the MWTM Client for Solaris page, select **Download Solaris Client**.

The web interface shows the supported Solaris versions and instructions for downloading the Solaris client. See the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for a detailed procedure.

To start the client after installation, add the `/opt/CSCOsgmClient/bin` subdirectory to your path, then enter the **mwtm client** command from the command line.

Downloading the Windows Client

To access the MWTM Client for Windows page, select **Download Windows Client**.

The web interface shows supported Windows versions and instructions for downloading the Windows setup program. After downloading the setup program onto your desktop or other Windows directory, double-click the **setup.exe** icon to start the setup program and launch the installation wizard. See the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for detailed procedures.

To start the client after installation, launch it from the Windows Start menu or double-click the **MWTM Client** icon on your desktop.

Downloading the Linux Client (Unsupported)

To access the MWTM Client for Linux page, select **Download Linux Client**.



Note

The MWTM does not support the MWTM client for Linux. Use the MWTM Linux client under advisement.

The web interface shows the supported Linux versions and instructions for downloading the Linux client. See the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for a detailed procedure.

To start the client after installation, add the `/opt/CSCOsgmClient/bin` subdirectory to your path, then enter the **mwtm client** command from the command line.

Checking Your Browser

MWTM 6.1 supports the following browsers:

Operating System	Supported Browsers
Windows	- Internet Explorer 6 - Internet Explorer 7 - Firefox 3.0¹
Solaris 9 Solaris 10	Firefox 2.0
Red Hat Enterprise Linux AS 4.0	

¹ The first time you attempt to connect to the MWTM server using Firefox 3.0, you must add an exception to allow the connection. See the MWTM 6.1 Release Notes for more information.



Note

Opening the MWTM in an unsupported browser generates a warning. Also, if JavaScript is not enabled, the MWTM web interface cannot function.

To check your browser and screen settings, select **Browser Checker**.

The Browser Checker window contains:

Pane or Field	Description
Browser Information:	
Browser	The name and version of the browser you are using. For example, Firefox 1.5.0.9.
Browser User Agent	Text string sent to identify the user agent to the server. Typically includes information such as the application name, version, host operating system, and language.
Platform	The platform type. For example, Win32.
Cookies Enabled	Whether you have cookies enabled on the browser (Yes or No).
Javascript Enabled	Whether Javascript is enabled (Yes or No).
AJAX Component	The Asynchronous JavaScript and XML (AJAX) component sends asynchronous HTTP update requests. The MWTM web application is only accessible to web browsers that have an AJAX component enabled. Typical values include XMLHttpRequest (for Mozilla-based browsers) and MSXML2.XmlHttp (for IE 6).
Screen Information:	
Size	Resolution of the display; for example, 1024 x 768.
Color Depth	Depth of the color display; for example, 16.

Accessing Software Updates and Additional Information

You can access this information about the MWTM from the MWTM web interface Home page. To:

- View information about the MWTM or any other Cisco product available on Cisco.com, select **Cisco Home Page**.
- Read Cisco literature associated with the MWTM, including product data sheets, Q and As, and helpful presentations, select **MWTM Home Page**.
- Access software updates for the MWTM from Cisco.com for FTP, select **Engineering Software Updates (FTP)**. The Cisco Systems Engineering FTP server page appears.

- Access software updates for the MWTM from Cisco.com, select **MWTM Software Download Page**. The Software Download page for the MWTM appears.
- Access the most recent versions of customer documentation for the MWTM, select **Latest MWTM Documentation**. The Cisco Mobile Wireless Transport Manager documentation page on Cisco.com appears. From this page, you can view the latest versions of MWTM release notes, installation guides, and end-user guides.

**Note**

If you cannot access Cisco.com from your location, you can always view the customer documentation that was delivered with the MWTM software. See the “[Viewing the MWTM Technical Documentation](#)” section on page 11-12.

Viewing the MWTM Technical Documentation

From the MWTM web interface Home page, you can view this MWTM technical documentation. To view the:

- Entire Cisco Mobile Wireless Transport Manager Help System, select **Help Home Page**.
- Entire *User Guide for the Cisco Mobile Wireless Transport Manager 6.1* as a PDF file on the web, using the Adobe Acrobat Reader, select **User Guide (PDF)**.
- Entire *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* as a PDF file on the web, using the Adobe Acrobat Reader, select **Install Guide (PDF)**.
- Entire *Release Notes for the Cisco Mobile Wireless Transport Manager 6.1* as a PDF file on the web, using the Adobe Acrobat Reader, select **Release Notes (PDF)**.
- Frequently Asked Questions (FAQs) about the MWTM, select **Frequently Asked Questions**.
- Syntax for every MWTM command, select **MWTM Server Help Command**.

**Caution**

These PDF versions of technical documents might not be the latest versions. For the latest versions, go to: http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html.

Displaying the Administrative Page

The MWTM web interface Administrative page provides access to MWTM system information, including messages, logs, status, and properties.

To access the Administrative page of the MWTM web interface, click **Administrative** under the navigation tree in the left pane. The right pane displays the information indicated in [Table 11-1](#).

**Note**

If MWTM User-Based Access is enabled, only users with authentication level 3 (Network Operator) and higher can see all options. Users of all other levels see only the System Information and System Status panes.

Table 11-1 Administrative Page Information

Pane	GUI Elements	Description	Reference
System Information	• README • (ITP only) ITP OS README • (IPRAN only) IPRAN OS README • (mSEF, CSG1 only) CSG1 OS README • (mSEF, CSG2 only) CSG2 OS README • (mSEF, GGSN only) GGSN OS README • (mSEF, HA only) HA OS README • (mSEF, BWG only) BWG OS README • MIBs	• <i>README.txt</i> file • <i>MWTM-OS-Info-ITP</i> file • <i>MWTM-OS-Info-IPRAN</i> file • <i>MWTM-OS-Info-CSG1</i> file • <i>MWTM-OS-Info-CSG2</i> file • <i>MWTM-OS-Info-GGSN</i> file • <i>MWTM-OS-Info-HA</i> file • <i>MWTM-OS-Info-BWG</i> file • Lists of MIBs, which may include: – (IPRAN only) RAN MIBs – (ITP only) ITP MIBs – (mSEF only) CSG1 MIBs – (mSEF only) CSG2 MIBs – (mSEF only) GGSN MIBs – (mSEF only) BWG MIBs – (mSEF only) HA MIBs – Common MIBs	For details, see Viewing System Information for the MWTM , page 11-14.
System Messages	• Info Messages • Error Messages • User Actions • Message Archives	Shows tabular information about different types of system messages.	For details, see Viewing System Messages , page 11-16.

Table 11-1 Administrative Page Information (continued)

Pane	GUI Elements	Description	Reference
System Status	- System Status - System Versions - Connected Clients - User Accounts	Shows the output of these system commands: mwtm status mwtm version mwtm who mwtm users	For details, see Viewing System Status Information , page 11-20.
System Logs	- Console Log - Command Log - Event Automation Log - Security Log - Install Log - Web Access Log - Web Error Log - Report Log	Shows the contents of these system logs: <i>sgmConsoleLog.txt</i> <i>sgmCommandLog.txt</i> <i>eventAutomationLog.txt</i> <i>sgmSecurityLog.txt</i> <i>cisco_sgmsvr_install.log</i> <i>access_log</i> <i>error_log</i> <i>sgmReportLog.txt</i>	For details, see Viewing System Logs , page 11-22.
Properties	- System - Server - WebConfig - Reports - Trap Forwarding	Shows the contents of these system property files: <i>System.properties</i> <i>Server.properties</i> <i>WebConfig.properties</i> <i>Reports.properties</i> <i>TrapForwarder.properties</i>	For details, see Viewing System Properties , page 11-25.

Viewing System Information for the MWTM

Depending upon which type(s) of network you are managing, you can view this MWTM system information from the Administrative page:

- **README**—Shows the contents of the */opt/CSCOsgm/install/README.txt* file. This file provides a brief overview of the system requirements and the tasks that are necessary to install this software release.

To access the MWTM README page, choose **README** from the **Administrative** page.

- **(ITP only) ITP OS README**—Shows the contents of the */opt/CSCOsgm/install/MWTM-OS-Info-ITP* file. This file contains a list of the supported OS software images for:
 - ITP nodes
 - GTT encoding scheme
 - MLR address table configuration

- GTT accounting statistics reports
- Route table and GTT table deployment
- MSU rates
- ITP provisioning

To access the MWTM ITP OS README page, choose **ITP OS README** from the **Administrative** page.

- *(IPRAN only)* **IPRAN OS README**—Shows the contents of the `/opt/CSCOs/gm/install/MWTM-OS-Info-IPRAN` file. This file contains a list of the supported OS software images for:
 - MWR nodes
 - ONS nodes
 - RAN SVC cards

To access the MWTM IPRAN OS README page, choose **IPRAN OS README** from the **Administrative** page.

- *(mSEF, CSG1 only)* **CSG1 OS README**—Shows the contents of the `/opt/CSCOs/gm/install/MWTM-OS-Info-CSG` file. This file contains a list of the supported OS software images for CSG1.

To access the MWTM CSG1 OS README page, choose **CSG1 OS README** from the **Administrative** page.

- *(mSEF, CSG2 only)* **CSG2 OS README**—Shows the contents of the `/opt/CSCOs/gm/install/MWTM-OS-Info-CSG2` file. This file contains a list of the supported OS software images for CSG2.

To access the MWTM CSG2 OS README page, choose **CSG2 OS README** from the **Administrative** page.

- *(mSEF, GGSN only)* **GGSN OS README**—Shows the contents of the `/opt/CSCOs/gm/install/MWTM-OS-Info-GGSN` file. This file contains a list of the supported OS software images for GGSN.

To access the MWTM GGSN OS README page, choose **GGSN OS README** from the **Administrative** page.

- *(mSEF, HA only)* **HA OS README**—Shows the contents of the `/opt/CSCOs/gm/install/MWTM-OS-Info-HA` file. This file contains a list of the supported OS software images for HA.

To access the MWTM HA OS README page, choose **HA OS README** from the **Administrative** page.

- *(mSEF, BWG only)* **BWG OS README**—Shows the contents of the `/opt/CSCOs/gm/install/MWTM-OS-Info-BWG` file. This file contains a list of the supported OS software images for BWG.

To access the MWTM BWG OS README page, choose **BWG OS README** from the **Administrative** page.

- **MIBs**—Shows a list of the MIBs (categorized by product type) on the server to which you are connected, and which is currently running the MWTM.

Each MIB appears in a list as a clickable link. You can open or download the contents of the MIB by clicking the MIB name. See [Appendix F, “MIB Reference,”](#) for a complete list and high-level description of each supported MIB.

To access the MIBs page, choose **MIBs** from the **Administrative** page of the MWTM web interface.

Viewing System Messages

You can view these MWTM system messages from the Administrative page:



Note

These messages are related to the MWTM system itself, not to your network.

- [Viewing Info Messages, page 11-16](#)
- [Viewing Error Messages, page 11-16](#)
- [Viewing MWTM User Action Messages, page 11-17](#)
- [Viewing All Archived MWTM Messages, page 11-19](#)

Viewing Info Messages

The System Messages: Last *number* Info Messages page shows informational messages in the MWTM system log. These messages can be useful when diagnosing and correcting MWTM operational problems.

To access this page, click **Info Messages** from the **Administrative** page, or **Info** from the web page menu bar, if visible.

The Last Info Messages table contains:

Column	Description
Period (in heading)	Collection period of the table, such as <code>Since Server Restart</code> .
Timestamp (in heading)	Date and time the MWTM last updated the information on the page.
Row	Unique number identifying each entry in the table. You cannot edit this field.
Time	Date and time the message was logged. To sort the messages by time, click the Time heading.
Source	Source for the message, with the format <i>process.host.id</i> , where: • <i>process</i> is the process that logged the message. • <i>host</i> is the host name of the process that logged the message. • <i>id</i> is an MWTM ID that uniquely identifies the process that logged the message; or in the event that two or more clients are running on the same node, connected to the same MWTM server.
Task	Task, or thread, that logged the message.
Message	Text of the message. To sort the messages alphabetically by message text, click the Message heading.

Viewing Error Messages

The System Messages: Last *number* Error Messages page shows error messages stored in the MWTM system log. These messages can be useful when diagnosing and correcting MWTM operational problems.

To access this page, click:

- **Error Messages** from the Administrative page.
- **Error** from the web page menu bar, if visible.

The Last Error Messages table contains:

Column	Description
Period (in heading)	Collection period of the table, such as <code>Since Server Restart</code> .
Timestamp (in heading)	Date and time the MWTM last updated the information on the page.
Row	Unique number identifying each entry in the table. You cannot edit this field.
Time	Date and time the message was logged. To sort the messages by time, click the Time heading.
Source	Source for the message, with the format <i>process.host.id</i> , where: • <i>process</i> is the process that logged the message. • <i>host</i> is the host name of the process that logged the message. • <i>id</i> is an MWTM ID that uniquely identifies the process that logged the message; or in the event that two or more clients are running on the same node, connected to the same MWTM server.
Task	Task, or thread, that logged the message.
Message	Text of the message. To sort the messages alphabetically by message text, click the Message heading.

Viewing MWTM User Action Messages

The System Messages: Last *number* Action Messages page shows user action messages stored in the MWTM system log. These messages can be useful when diagnosing and correcting MWTM operational problems, and when monitoring audit trails of user actions.

To access this page, use one of these procedures. Click:

- **User Actions** from the Administrative page.
- **Action** from the web page menu bar, if visible.

The MWTM shows the System Messages: Last *number* Action Messages page. The System Messages: Last *number* Action Messages page has these sections:

- [Last Action Messages Menu, page 11-18](#)
- [Last Action Messages Table, page 11-18](#)

Last Action Messages Menu

By default, the MWTM shows action messages of all classes on the System Messages: Last *number* Action Messages page. However, the MWTM provides menu options that enable you to display only messages of a specific class on the page.

The Last Action Messages menu contains:

Column	Description
Create	Opens the System Messages: Last <i>number</i> Action: specified web page:
Delete	• Create—Opens the Create Messages web page, showing only Create action messages. • Delete—Opens the Delete Messages web page, showing only Delete action messages. • Discover—Opens the Discover Messages web page, showing only Discover action messages. • Edit—Opens the Edit Messages web page, showing only Edit action messages. • Ignore—Opens the Ignore Messages web page, showing only Ignore action messages.
Discover	
Edit	
Ignore	
OverWrite	
Poll	• OverWrite—Opens the OverWrite Messages web page, showing only OverWrite action messages. • Poll—Opens the Poll Messages web page, showing only Poll action messages. • Purge—Opens the Purge Messages web page, showing only Purge action messages. • LogInOut—Opens the LogInOut Messages web page, showing only Log in and Log out action messages. • All—Opens a web page that shows all action messages. • Provision—Opens a web page that shows all provisioning messages.
Purge	
LogInOut	
All	
Provision	

Last Action Messages Table

The Last Action Messages table contains:

Column	Description
Period (in heading)	Collection period of the table, such as Since Server Restart.
Timestamp (in heading)	Date and time the information on the page was last updated by the MWTM.
Row	Unique number identifying each entry in the table. You cannot edit this field.
Time	Date and time the message was logged. To sort the messages by time, click the Time heading.

Column	Description
Class	Class of the message. Possible classes are: • Create—Creation event, such as the creation of a seed file. • Delete—Deletion event, such as the deletion of an object or file. • Discover—Discovery event, such as Discovery beginning. • Edit—Edit event. A user has edited an object. • Ignore—Ignore event. A user has flagged a link or linkset as Ignored. • Login—Login event. A user has logged in to the MWTM. • LoginDisable—LoginDisable event. The MWTM has disabled a user's User-Based Access authentication as a result of too many failed attempts to log in to the MWTM. • LoginFail—LoginFail event. An attempt by a user to log in to the MWTM has failed. • Logout—Logout event. A user has logged out of the MWTM. • OverWrite—OverWrite event. An existing file, such as a seed file or route file, has been overwritten. • Poll—Poll event, such as an SNMP poll. • Purge—Purge event. A user has requested Discovery with Delete Existing Data chosen, and the MWTM has deleted the existing MWTM database. To sort the messages by class, click the Class heading.
Message	Text of the message. To sort the messages alphabetically by message text, click the Message heading.

Viewing All Archived MWTM Messages

The System Message Archives: All Messages page shows all archived messages in the MWTM system logs, including:

- error
- informational
- trace
- debug
- dump
- messages
- SNMP

To access the System Message Archives: All Messages page, use one of these options. Click:

- **Message Archives** from the Administrative page.
- **Archives** from the web page menu bar, if visible.

On the System Message Archives: All Messages page, messages are archived by timestamp. Each archived file contains all MWTM system messages for a single session for the server to which you are connected, and which is currently running the MWTM server. (If you restart the server, the MWTM creates a new file.)

To view archived messages, click a timestamp. The System Messages Archive: Last *number* All Messages page appears, which shows all messages that were in the system log at the specified timestamp.

**Note**

You might observe an entry labeled *messageLog-old* among a list of files that have timestamps in the filenames. A daily cron job creates the files with the timestamps. The cron job, which runs at midnight, searches through the *messageLog.txt* and *messageLog-old.txt* files for all entries from the past day. The *messageLog-old.txt* file exists only if the size of *messageLog.txt* exceeds the limit set by the [mwtm logsize](#) command. The MWTM lists the contents of *messageLog-old.txt* because it could contain important data from the day the message log file rolled over.

The Last All Messages table contains this information (without column headers):

Description	Information
Index	Message number that the MWTM assigns to the message.
Time	Date and time the message was logged.
Type	Type of message. Possible types are: • Action • Debug • Dump • Error • Info • SNMP • Trace
Source	Source for the message, with the format <i>process.host.id</i> , where: • <i>process</i> is the process that logged the message. • <i>host</i> is the host name of the process that logged the message. • <i>id</i> is an MWTM ID that uniquely identifies the process that logged the message; or, in the event that two or more clients are running on the same node, connected to the same MWTM server.
Task	Task, or thread, that logged the message.
Message	Text of the message.

Viewing System Status Information

You can view this MWTM system status information from the Administrative page:

- [Viewing System Status, page 11-21](#)
- [Viewing System Versions, page 11-21](#)
- [Viewing Connected Clients, page 11-21](#)
- [Viewing User Accounts, page 11-21](#)

Viewing System Status

To access system status information, click **System Status** from the Administrative page. (The MWTM might take a few seconds to display this page.) This page shows the status of all MWTM servers, local clients, and processes.

Viewing System Versions

To access version information, click **System Versions** from the Administrative page. (The MWTM might take a few seconds to display this page.) This page shows version information for all MWTM servers, clients, and processes.

Viewing Connected Clients

To access connected client information, click **Connected Clients** from the Administrative page. This page lists all MWTM clients that are currently connected to the MWTM server. It also lists all Solaris and Linux users that are logged in to the MWTM server.

Viewing User Accounts

To access user account information, click **User Accounts** from the Administrative page. This page shows information about all user accounts that have been defined for the MWTM server. If no user accounts have been defined, the MWTM shows this message:

```
User Database is Empty
```

The user accounts page displays the output of the **mwtm users** command. For example:

```
/opt/CSC0sgm/bin/mwtm users
```

```
User Name Last Login                               Level Name & Number Status
-----
User1      Wed Jan 17 14:03:13 EST 2007 System Admin    5  [Account Enabled]
User2      Unknown                               System Admin    5  [Account Enabled]
User3      Wed Jan 17 13:43:30 EST 2007 System Admin    5  [Account Enabled]
```

```
User Based Access Protection is Enabled.
```

```
Authentication type = local
```

The the **mwtm users** command output contains:

Heading	Description
User Name	The MWTM user for whom a User-Based Access account has been set up.
Last Login	Date and time the user last logged in to the MWTM.

Heading	Description
Level Name & Number	Authentication level and number for the user. Valid levels and numbers are: • Basic User, 1 • Power User, 2 • Network Operator, 3 • Network Administrator, 4 • System Administrator, 5
Status	Current status of the user's account. Valid status settings are: • Account Enabled—The account has been enabled and is functioning normally. • Account Disabled—The account has been disabled for one of these reasons: – A System Administrator disabled the account. See the “mwtm disablepass” section on page B-25 and the “mwtm disableuser” section on page B-26 for more information. – The MWTM disabled the account as a result of too many failed attempts to log in using the account. See the “mwtm badlogindisable” section on page B-11 for more information. – The MWTM disabled the account because it was inactive for too many days. See the “mwtm inactiveuserdays” section on page B-32 for more information.

Viewing System Logs

From the Administrative page, you can view:

- [Viewing the Console Log, page 11-22](#)
- [Viewing the Command Log, page 11-23](#)
- [Viewing the Event Automation Log, page 11-23](#)
- [Viewing the Security Log, page 11-23](#)
- [Viewing the Install Log, page 11-24](#)
- [Viewing the Web Access Logs, page 11-24](#)
- [Viewing the Web Error Logs, page 11-24](#)
- [Viewing the Report Log, page 11-25](#)

Viewing the Console Log

The Console Log shows the contents of the MWTM system console log file for the server to which you are connected, and which is currently running the MWTM. The console log file contains unexpected error and warning messages from the MWTM server, such as those that might occur if the MWTM server cannot start. It also provides a history of start-up messages for server processes and the time each message appeared.

To access the Console Log, click **Console Log** in the System Logs pane of the Administrative page. You can also view the Console Log with the [mwtm console](#) command.

Viewing the Command Log

The Command Log shows the contents of the MWTM system command log file for the server to which you are connected, and which is currently running the MWTM server. The system command log lists all **mwtm** commands that have been entered for the MWTM server, the time each command was entered, and the user who entered the command.

To access the Command Log, click **Command Log** in the System Logs pane of the Administrative page. You can also view the Command Log with the **mwtm cmdlog** command.

The MWTM Command Log page appears. The Command Log table contains:

Column	Description
Timestamp	Date and time the command was logged. To sort the messages by time, click the Timestamp heading.
User	User who entered the command. To sort the commands by user, click the User heading.
Command	Text of the command. To sort the messages alphabetically by command text, click the Command heading.

Viewing the Event Automation Log

The Event Automation Log shows the contents of the system event automation log file for the server to which you are connected, and which is currently running the MWTM server. The system event automation log lists all messages that event automation scripts generate.

The default path and filename for the system event automation log file is */opt/CSCOsgm/logs/eventAutomationLog.txt*. If you installed the MWTM in a directory other than */opt*, then the system event automation log file is in that directory.

To access the Event Automation Log, click **Event Automation Log** in the System Logs pane of the Administrative page. You can also view the Event Automation Log with the **mwtm eventautolog** command.

Related Topic

[Changing the Way the MWTM Processes Events, page 9-35.](#)

Viewing the Security Log

The Security Log shows the contents of the MWTM system security log file for the server to which you are connected, and which is currently running the MWTM server. The system security log lists:

- All security events that have occurred for the MWTM server
- The time each event occurred
- The user and command that triggered the event
- The text of any associated message

The default path and filename for the system security log file is */opt/CSCOsgm/logs/sgmSecurityLog.txt*. If you installed the MWTM in a directory other than */opt*, then the system security log file is in that directory.

To access the Security Log, click **Security Log** in the System Logs pane of the Administrative page. You can also view the Security Log with the `mwtm seclog` command.

The Last Security Entries table contains these columns:

Column	Description
Timestamp	Date and time the security event occurred. To sort the entries by time, click the Time heading.
User	User who triggered the security event. To sort the entries by user, click the User heading.
Message	Text of the security event message. To sort the entries alphabetically by message text, click the Message heading.
Command	Text of the command that triggered the security event. To sort the entries alphabetically by command text, click the Command heading.

Viewing the Install Log

The Install Log shows the contents of the MWTM system installation log. The installation log contains messages and other information recorded during installation, which can be useful when troubleshooting problems. The Install Log also records the installer's selections (for example, whether the installer chose to configure the MWTM to receive SNMP traps).

The default path and filename for the install log file is `/opt/CSCOs/gm/install/cisco_sgmsvr_install.log`. If you installed the MWTM in a directory other than `/opt`, then the install log file is in that directory.

To access the Install Log, click **Install Log** in the System Logs pane of the Administrative page. You can also view the Install Log with the `mwtm installlog` command.

Viewing the Web Access Logs

The Web Access Logs page shows a list of web access log files for the server to which you are connected, and which is currently running the MWTM server. The web access log lists all system web access messages that have been logged for the MWTM server, providing an audit trail of all access to the MWTM server through the MWTM web interface.

The default path and filename for the web access log file is `/opt/CSCOs/gm/apache/logs/access_log`. If you installed the MWTM in a directory other than `/opt`, then the web access log file is in that directory.

To access the Web Access Logs page, click **Web Access Logs** from within the System Logs pane of the Administrative page. You can also view the Web Access Logs page using the `mwtm webaccesslog` command.

Viewing the Web Error Logs

The Web Error Logs page shows a list of web error log files for the server to which you are connected, and which is currently running the MWTM server. The web server error log lists all system web error messages that have been logged for the MWTM web server. You can use the web error log to troubleshoot the source of problems that users may have encountered while navigating the MWTM web interface.

The default path and filename for the web error log file is `/opt/CSCOs/gm/apache/logs/error_log`. If you installed the MWTM in a directory other than `/opt`, then the web error log file is in that directory.

To access the Web Error Logs page, click **Web Error Logs** in the System Logs pane of the Administrative page. You can also view the Web Error Logs page using the `mwtm weberrorlog` command.

Viewing the Report Log

The Report Log shows the message log for ITP reports for the server to which you are connected, and which is currently running the MWTM server. You can view this log to determine the beginning and finish times for report generation. The log also records errors that occurred during report generation (for example, server connection errors).

The default path and filename for the report log file is `/opt/CSCOs/gm/logs/sgmReportLog.txt`. If you installed the MWTM in a directory other than `/opt`, then the report log file is in that directory.

To access the Report Log, click **Report Log** in the System Logs pane of the Administrative page. You can also view the Report Log with the `mwtm replog` command.

Viewing Properties

Property files for the MWTM are in the `/opt/CSCOs/gm/properties` directory. You can view these MWTM properties from the Administrative page.

- [Viewing System Properties, page 11-25](#)
- [Viewing Server Properties, page 11-27](#)
- [Viewing Web Configuration Properties, page 11-27](#)
- [Viewing Reports Properties, page 11-29](#)
- [Viewing Trap Forwarding Properties, page 11-30](#)

Viewing System Properties

To access the System Properties file, click **System** in the Properties pane of the Administrative page. The MWTM shows the contents of the `/opt/CSCOs/gm/properties/System.properties` file.

The System Properties file contains MWTM server and client properties that control various MWTM configuration parameters.

You can change some of the system properties using MWTM commands:

To change this system property	Use this MWTM command
ATBLDIR	<code>mwtm atbldir</code> , page B-90
AUTO_SYNC_CONFIG	<code>mwtm autosynconfig</code> , page B-91
BACKUP_RMIPORT	<code>mwtm secondaryserver</code> , page B-56
BACKUP_SERVER	
BACKUP_WEBPORT	
BACKUPDAYS	<code>mwtm backupdays</code> , page B-9
BADLOGIN_TRIES_ALARM	<code>mwtm badloginalarm</code> , page B-11

To change this system property	Use this MWTM command
BADLOGIN_TRIES_DISABLE	mwtm badlogindisable, page B-11
CHART_MAX_WINDOW	mwtm chartwindow, page B-91
CONSOLE_ARCHIVE_DIR_MAX_SIZE	mwtm archivedirsize, page B-8
CONSOLE_LOG_MAX_SIZE	mwtm consolelogsize, page B-20
CSV_FIELD_DELIMITER	mwtm collectstats, page B-19
CSV_STRING_DELIMITER	
CW2K_SERVER	mwtm cwsetup, page B-21
CW2K_WEB_PORT	
CW2K_SECURE_WEB_PORT	
GTTDIR	mwtm gttdir, page B-98
JSP_PORT	mwtm jspport, page B-36
LOGAGE	mwtm msglogage, page B-45
LOGDIR	mwtm msglogdir, page B-46
LOGSIZE	mwtm logsize, page B-39
LOGTIMEMODE	mwtm logtimemode, page B-40
LOG_TROUBLESHOOTING	mwtm tshootlog, page B-77
MANAGE_BWG	mwtm manage, page B-40
MANAGE_CSG1	
MANAGE_CSG2	
MANAGE_GGSN	
MANAGE_HA	
MANAGE_ITP	
MANAGE_RAN-O	
PERSISTENCEDIR	mwtm datadir, page B-22
PROMPT_CREDS	mwtm logincreds, page B-38
REQUIRE_ARCHIVE_COMMENTS	mwtm deploycomments, page B-95
ROUTEDIR	mwtm routedir, page B-114
SBACKUPDIR	mwtm backupdir, page B-10
SERVER_NAME	mwtm servername, page B-57
SNMPCONFFILE	mwtm snmpconf, page B-60
SSL_ENABLE	mwtm ssl, page B-70
TFTP_ATBLPATH	mwtm atbldir, page B-90
TFTP_GTTTPATH	mwtm gttdir, page B-98
TFTP_ROUTEPAH	mwtm routedir, page B-114
TRAP_LIST_ENABLE	mwtm trapsetup, page B-76
TRAP_PORT	
USE_TERMINAL_PROXY	mwtm termproxy, page B-75

To change this system property	Use this MWTM command
VCS_REPOSITORY_DIR	mwtm archivedir, page B-88
WEB_PORT	mwtm webport, page B-83
WEB_BROWSER	mwtm browserpath, page B-12

For these system properties, you can view related documentation:

System Property	Related Documentation
CLIENT_PORT	Configuring Port Numbers and Parameters, page H-7
DATASERVER_PORT	
LOGINSERVER_PORT	
RMIREGISTRY_PORT	
MAX_CHART_SERIES	Viewing Backhaul Performance Data, page 8-111

Viewing Server Properties

To access the Server Properties file, click **Server** in the Properties pane of the Administrative page. The MWTM shows the contents of the */opt/CSCOs/gm/properties/Server.properties* file.

The Server Properties file contains various properties that control the MWTM server.

You can use MWTM commands to change these server properties:

To change this server property	Use this MWTM command
DEMAND_POLLER_TIMELIMIT	mwtm pollertimeout, page B-49
SNMP_MAX_ROWS	mwtm snmpwalk, page B-66
UNKNOWN_AGING_TIMEOUT	mwtm unknownage, page B-78

To change poller parameters in the Server Properties file, see the “[Changing MWTM Server Poller Settings](#)” section on [page 3-2](#).

Viewing Web Configuration Properties

To access the Web Configuration Properties file, click **WebConfig** in the Properties pane of the Administrative page. The MWTM shows the contents of the */opt/CSCOs/gm/properties/WebConfig.properties* file.

The Web Configuration Properties file contains properties that control the configuration of the MWTM web interface. For example:

```
MAX_ASCII_ROWS      = 6000
MAX_HTML_ROWS       = 100

# The selectable page sizes start at MIN_SELECTABLE_PAGE_SIZE and doubles until
# the MAX_SELECTABLE_PAGE_SIZE value is reached
# (e.g. 25, 50, 100, 200, 400, 800)
MIN_SELECTABLE_PAGE_SIZE = 25
MAX_SELECTABLE_PAGE_SIZE = 800
LOG_UPDATE_INTERVAL = 300
```

```

WEB_UTIL          = percent
WEB_NAMES         = display
MAX_EV_HIST       = 15000

```

You can use the MWTM to change the web configuration properties:

Web Configuration Property	Changing Default Setting
LOG_UPDATE_INTERVAL	To control how often, in seconds, the MWTM updates certain web output, use the mwtm weblogupdate command. The valid range is 1 second to an unlimited number of seconds. The default value is 300 seconds (5 minutes).
MAX_ASCII_ROWS	To set the maximum number of rows for MWTM ASCII web output, such as displays of detailed debugging information, use the mwtm maxasciirows command. The valid range is 1 row to an unlimited number of rows. The default value is 6,000 rows.
MAX_EV_HIST	To set the maximum number of rows for MWTM to search in the event history logs, use the mwtm maxevhist command. The event history logs are the current and archived MWTM network status logs for status change and SNMP trap messages. The MWTM sends the results of the search to the web browser, where the results are further limited by the setting of the mwtm maxhtmlrows command. The valid range is 1 row to an unlimited number of rows. The default value is 15,000 rows.
MAX_HTML_ROWS	To set the maximum number of rows for MWTM HTML web output, such as displays of statistics reports, status change messages, or SNMP trap messages, use the mwtm maxhtmlrows command. This lets you select a page size (if you have not explicitly chosen a page size). Once you select a page size from any page, the MWTM remembers your preference until you delete your browser cookies. The default value is 100 rows.
MIN_SELECTABLE_PAGE_SIZE	This setting determines the minimum page size for the user to select from the Page Size drop-down menu. The page size values start with the MIN_SELECTABLE_PAGE_SIZE and double until they reach the MAX_SELECTABLE_PAGE_SIZE.
MAX_SELECTABLE_PAGE_SIZE	This setting determines the maximum page size for the user to select from the Page Size drop-down menu. The page size values start with the MIN_SELECTABLE_PAGE_SIZE and double until they reach the MAX_SELECTABLE_PAGE_SIZE.

Web Configuration Property	Changing Default Setting
WEB_NAMES	To specify whether the MWTM should show real DNS names or display names in web pages, enter the mwtm webnames command. To show: - The real DNS names of nodes, as discovered by the MWTM, enter mwtm webnames real. - Display names, enter mwtm webnames display. Display names are new names that you specify for nodes. This is the default setting. For more information about display names, see the “Editing Properties” section on page 6-33.
WEB_UTIL	To specify whether the MWTM should display send and receive utilization as percentages or in Erlangs in web pages, enter the mwtm who command. To show: - Utilization as a percentage, enter mwtm webutil percent. This is the default setting. - Display utilization in Erlangs (E), enter mwtm webutil erlangs. See Viewing RAN-O Performance Data, page 8-107 and Viewing RAN-O Error Data, page 8-115 for more information on send and receive utilization for shorthauls and backhauls. See Chapter 12, “Managing Reports” for more information on send and receive utilization for linksets and links.

Each of the web configuration commands requires you to be logged in as the root user, as described in the [“Becoming the Root User \(Server Only\)” section on page 4-2](#), or as a superuser, as described in the [“Specifying a Super User \(Server Only\)” section on page 2-20](#).

Related Topic

[Link Reports, page 12-17.](#)

Viewing Reports Properties

To access the Reports Properties file, click **Reports** in the Properties pane of the Administrative page. The MWTM shows the contents of the `/opt/CSCOsgm/properties/Reports.properties` file.

The Reports Properties file contains properties that control various aspects of the reports that are available in the MWTM web interface.

You can use MWTM commands to change these reports properties:

To change this server property	Use this MWTM command
ACC_REPORTS	mwtm accstats, page B-87
GTT_REPORTS	mwtm gttstats, page B-100
LINK_REPORTS	mwtm linkstats, page B-101
MLR_REPORTS	mwtm mlrstats, page B-105
MSU_REPORTS	mwtm statreps msu, page B-124
Q752_REPORTS	mwtm q752stats, page B-110
RPT_15MIN_AGE	mwtm rep15minage, page B-130

To change this server property	Use this MWTM command
RPT_CUSTOM_AGE	mwtm repcustage, page B-112
RPT_DAILY_AGE	mwtm repdailyage, page B-52
RPT_HOURLY_AGE	mwtm rephourlyage, page B-53
RPT_IPLINKS	mwtm statreps iplinks, page B-122
RPT_MONTHLY_AGE	mwtm restart, page B-53
RPT_NULLCAPS	mwtm statreps nullcaps, page B-125
RPT_SERVRATIO	mwtm statreps servratio, page B-126
RPT_TIMEMODE	mwtm statreps timemode, page B-127
STATS_REPORTS	mwtm statreps servratio, page B-126
XUA_REPORTS	mwtm xuastats, page B-129

Viewing Trap Forwarding Properties

To access the Trap Forwarding Properties file, click **TrapForwarding** in the Properties pane of the Administrative page. The MWTM shows the contents of the */opt/CSCOs/sgm/properties/TrapForwarder.properties* file.

The Trap Forwarder Properties file contains a list of the destination addresses for the trap forwarder. Enter each destination address on its own line and use this format:

SERVER*xx*=*destination_IP_address*[:*port_number*]

The *port_number* parameter is optional.

Displaying Alarms and Events

To display alarms in the web interface, click Active Alarms in the navigation tree, or select an object in the navigation tree and click the Alarms tab.

To display events in the web interface, click Event History in the navigation tree, or select an object in the navigation tree and click the Recent Events tab.

Viewing alarms and events in the web interface is essentially the same as viewing them in the MWTM client. Only minor differences exist:

- A paging feature for paging through large tables.
- A refresh interval that you can change.
- An Archived link for viewing archived alarms.
- Alarm selection by check box and a Clear Selection link.
- Severity drop-down list and a Change Severity button.

For detailed descriptions of these tools, see the [“Using the Toolbar” section on page 11-5](#)

For descriptions of the columns, see the [“Right-click Menus” section on page 9-16](#).

Displaying Summary Lists

Displaying Summary Lists in the web interface is essentially the same as displaying them in the MWTM client. Only minor differences exist. Clicking on an object under the Summary Lists in the web interface causes the content area to show information about the object.

For details on:

- Navigating table columns, see [Navigating Table Columns, page 5-24](#).
- The toolbar, see [Using the Toolbar, page 11-5](#).

For complete information about Summary Lists, see the “[Displaying Object Windows](#)” section on [page 6-2](#).

Displaying Software Versions

The Software Versions table lists the software versions for each node the MWTM manages.

To access the Software Versions page:

- From the Web interface navigation tree, select **Summary Lists > Software Versions**.
- From the MWTM main window, select **View > Web > Software Versions**.

For details on:

- Navigating the columns of the Software Versions table, see [Navigating Table Columns, page 5-24](#).
- The toolbar, see [Using the Toolbar, page 11-5](#).

The Software Versions table contains:

Column	Description
Name	Name of the node.
Node Type	Type of node.
Software Version	Software version used by the node.
Software Description	Full software version information.

Tools

To access launch and search tools, click **Tools** in the navigation tree of the MWTM web interface. This action opens a Launch pane and a Search pane in the content area:

- [Launch Tools, page 11-32](#)
- [Search Tools, page 11-32](#)

Launch Tools

If you have integrated with a CiscoWorks server, one or more of the following applications appears in the Launch pane as active links:

- CiscoView
- CiscoWorks LMS Portal
- CSG Service Manager
- Device Center
- GGSN Service Manager

The name of the server appears in parentheses following the application names. To launch an application, click the application name. See [Integrating the MWTM with Other Products, page 5-39](#).



Note

The MWTM attempts to launch the URL of the service manager that resides on the LMS server. If the service manager is not installed on the LMS server, you will receive an HTTP 404 error. To prevent this error, ensure that the service managers are installed on the LMS server, or remove the CSG or GGSN network setting with the [mwtm manage, page B-40](#), command.

Search Tools



Note

You must have the Cisco Home Agent (HA) network enabled to use this tool (for details on enabling HA, see [mwtm manage, page B-40](#)).

The Search pane provides a tool that you use to search for a specific subscriber across one or more designated Cisco Home Agent (HA) routers. This tool is useful for troubleshooting problems that HA subscribers may report. To search for an HA subscriber:

- Step 1** Click **Search for Home Agent Subscriber** in the Search pane.
- Step 2** Click the Identifier Type radio button:
 - **Network Access Identifier**—Use this option if you know the subscriber's network access identifier (NAI); for example, jdoe@xyz.com.
 - **IP Address**—Use this option if you know the subscriber's IP address
- Step 3** Depending on your selection in [Step 2](#), enter the subscriber's NAI or IP address in the Mobile Node Identifier field.
- Step 4** In the Select Home Agents to Search pane, check the check boxes of the Home Agents that you want to search. (The default setting is all Home Agents.)
- Step 5** To conduct the search, click the **Search** button.
The Search Results popup window appears.
- Step 6** If the search successfully locates the subscriber, and you want to troubleshoot the problem, click the **Troubleshoot Subscriber** button in the Search Results popup.
The MWTM automatically navigates to the Troubleshooting tab of the HA device.

- Step 7** For more information about troubleshooting devices by using the Troubleshooting tab, see [Viewing Troubleshooting, page 8-43](#).
-

Displaying Reports

**Note**

If MWTM User-Based Access is enabled, only users with authentication level 4 (Network Administrator) and higher can see the Reports menu.

You can display reports primarily for ITP objects in the MWTM Web interface. An overview and a complete list and description of these reports is available in [Chapter 12, “Managing Reports.”](#)

Event reports are also available for both RAN-O and ITP networks, also available in the Reports menu. For details, see the [“Viewing Archived Event Files on the Web”](#) section on page 9-30 and the [“Viewing the Event Metrics Report on the Web”](#) section on page 9-30.

You can also display network-wide RAN-O reports in the Reports menu. For details, see [Viewing RAN Reports, page 12-75](#).

Displaying Objects in a View

Displaying objects in a view in the MWTM web interface is essentially the same as viewing them in the MWTM client. Only minor differences exist. The MWTM web interface:

- Shows a subset of the columns that the client interface shows.
- Has a paging feature. See the [“Using the Toolbar”](#) section on page 11-5.
- Has a refresh interval that you can change.
- Displays a Statistics tab when you select a CSG2 or BWG Gateway node in the navigation tree. See [Displaying CSG2 Real-Time Statistics, page 11-44](#), or [Displaying BWG Real-Time Statistics, page 11-49](#). The Statistics tab appears only on the web interface for these node types.
- When viewing CPU Utilization in the Performance tab, the MWTM web interface displays the data in tabular format instead of graph format. See [CPU Utilization, page 8-59](#).
- When viewing performance and error information for interfaces (in the Interface Performance and Interface Errors tabs), the MWTM web interface displays the data in tabular format only. The MWTM client interface displays the data in tabular and graph format. See [Viewing Data for Interfaces, page 8-63](#).

For details on each object type, see the [“Displaying Object Windows”](#) section on page 6-2.

Displaying RAN-O Historical Statistics

The MWTM web interface provides access to RAN-O historical statistics in the MWTM database. You can use these statistics for capacity planning and trend analysis. For example, you can generate graphs, tables, or CSV files:

- For a specified time range to display historical statistics for customer busy-hours.

- To show the maximum send and receive traffic over a specified time period.
- To show data on a 15-minute, daily, or hourly basis.

Using this information, you can perform detailed analysis of historical traffic utilization on the backhaul and shorthaul links to plan future facility upgrades.

**Note**

The MWTM client provides real-time (not historical) graphs depicting performance and error information occurring in real time. You use real-time statistics for troubleshooting active problem areas in your network. See [Viewing RAN-O Performance Data, page 8-107](#) and [Viewing RAN-O Error Data, page 8-115](#).

This section provides information about:

- [Displaying Performance Statistics, page 11-34](#)
- [Displaying Error Statistics, page 11-39](#)
- [Generating RAN Data Export Files, page 11-43](#)

Displaying Performance Statistics

You can view performance data for a shorthaul or backhaul interface in the MWTM:

- Web interface by selecting a shorthaul or backhaul interface in the navigation tree and clicking the Shorthaul Performance or Performance tab in the right pane.
- Client interface by right-clicking a shorthaul or backhaul interface in the navigation tree and clicking Performance History.

**Note**

If the CISCO-IP-RAN-BACKHAUL-MIB on the node is not compliant with the MWTM, the MWTM issues the message:

MIB not compliant for reports

Install a version of IOS software on the node that is compatible with the MWTM. For a list of compatible IOS software, from the MWTM:

- Web interface, choose **Administrative > IPRAN OS README**.
- Client interface, choose **View > Web > Administrative**; then click **IPRAN OS README**.

The Performance tab shows one or more graphs depending on the type of report chosen. These graphs depict send and receive rates of optimized IP traffic over a specified time range. The graphs display the traffic in bits per second. Each data series shows maximum, minimum, and average rates of optimized traffic.

The Performance tab for a backhaul interface shows total rates for GSM and UMTS traffic, including total error rates.

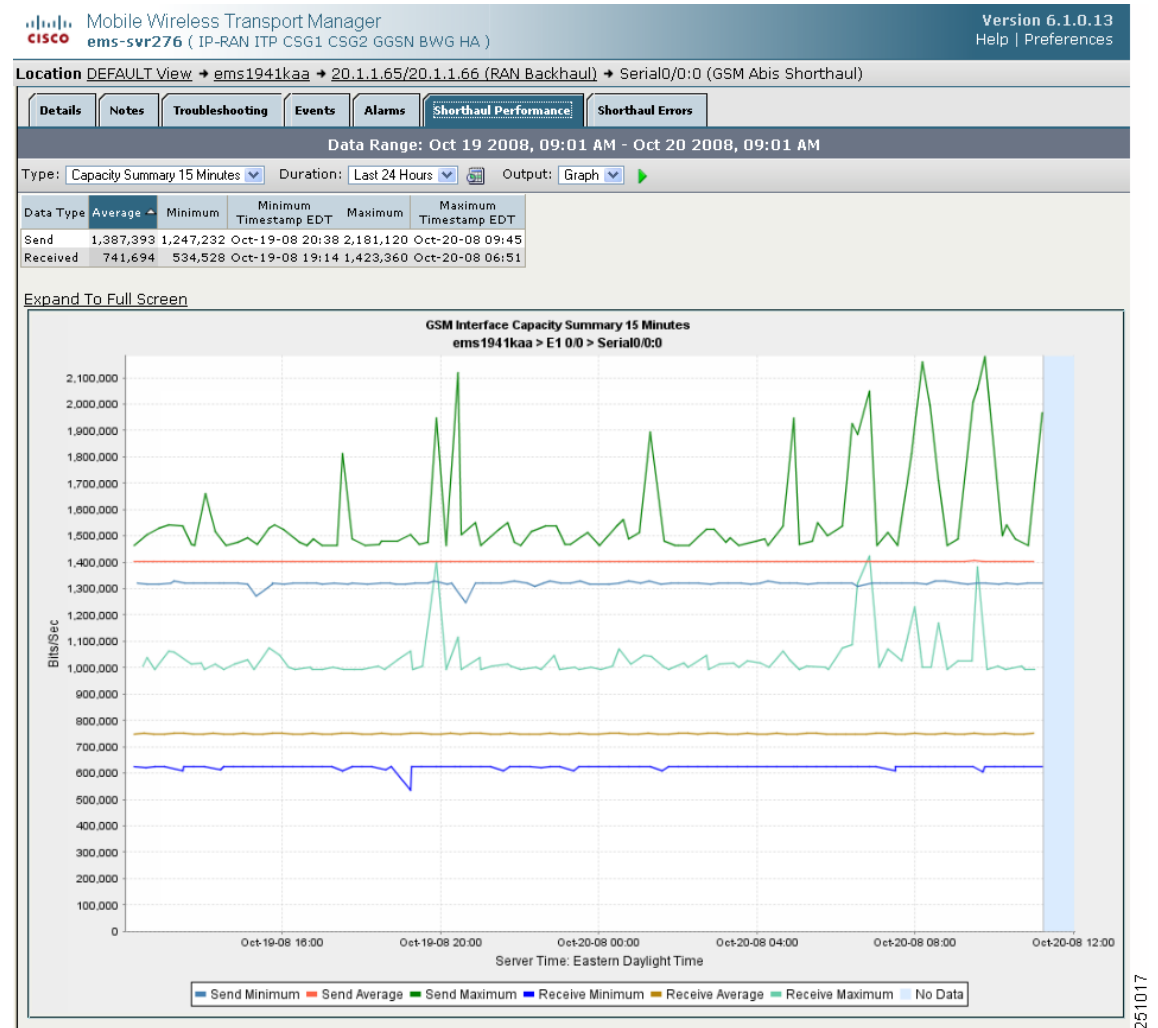
This section provides information about:

- [Displaying Shorthaul Performance Statistics, page 11-35](#)
- [Displaying Backhaul Performance Statistics, page 11-36](#)

Displaying Shorthaul Performance Statistics

The Shorthaul Performance tab for a shorthaul interface shows the maximum, minimum, and average rates for send and receive traffic.

Figure 11-2 Performance Tab for Shorthaul Interface



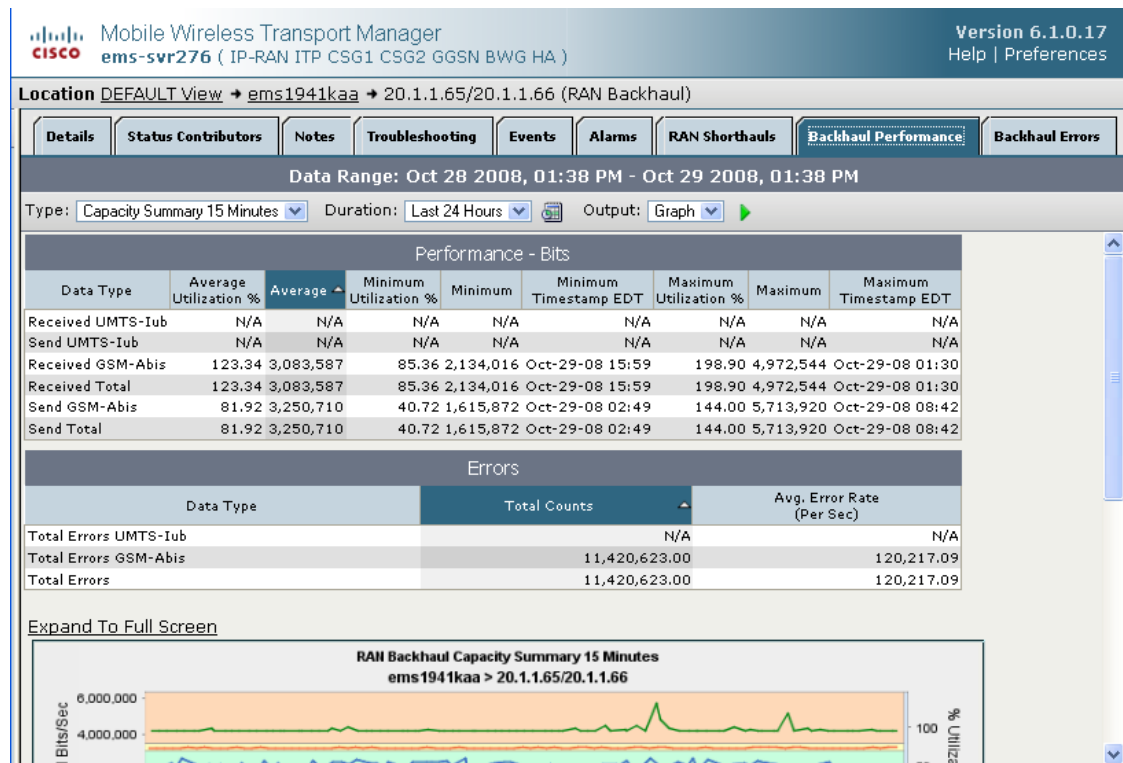
The Shorthaul Performance tab for a shorthaul interface contains:

GUI Element	Description
Toolbar	Provides functions to select a report type, duration, output type. See Using the Toolbar, page 11-5 .
Type	A comprehensive summary of minimum, average, and maximum capacity statistics for send and receive traffic on a RAN shorthaul. You can choose from 15-minute, hourly, or daily capacity summary reports, or choose a custom range.

GUI Element	Description
<i>Table</i>	If the Output Type is Graph, the table contains: • Data Type—Type of data, send or receive • Average—Average of the data across the chosen time range • Minimum—Minimum value across the chosen time range • Minimum Timestamp EDT—Time the minimum value occurred • Maximum—Maximum value across the chosen time range • Maximum Timestamp EDT—Time the maximum value occurred Note If the Output Type is Table or CSV, the same data is presented but the column headings are labeled by data type (for example, Send Average and Receive Average).
Expand to Full Screen	If Output Type is Graph, this text link that displays the graph in a new, full-screen window for easier viewing.
Bits/Sec	If Output Type is Graph, Y-axis label that shows traffic rate in bits per second. The Y axis automatically scales to the interface speed. Note If no data exists between any two data points, the graph displays a color-coded vertical bar to show the period for which no data is available.
Time	If Output Type is Graph, X-axis label that shows a historical time scale and the server time zone.
<i>Legend</i>	If Output Type is Graph, color-coded legend that shows labels for traffic rates.

Displaying Backhaul Performance Statistics

The Performance tab for a backhaul interface shows minimum, average, and maximum traffic rates for send and receive traffic. You can also determine the percentage of backhaul utilization that various traffic types occupy. Error rates appear, too.

Figure 11-3 Example of Performance Tab for Backhaul Interface

The Performance tab for a backhaul interface contains:

GUI Elements	Description
Toolbar	Provides functions to select a report type, duration, output type, and the Graph Series Editor. See the “Using the Toolbar” section on page 11-5 .
Type	Report Type. If you choose a Capacity Summary report, the report shows a comprehensive summary of minimum, average, and maximum capacity statistics for total traffic (GSM-Abis and UMTS-Iub), total GSM-Abis traffic, and total UMTS-Iub traffic. You can choose from 15-minute, hourly, or daily capacity summary reports. Error rates appear, too. If Output Type is Graph, statistics appear in three graphs: • Top—Capacity statistics for send traffic rates, including percentage of backhaul utilization (right side of graph). • Middle—Capacity statistics for receive traffic rates, including percentage of backhaul utilization (right side of graph). • Bottom—Error counts for send and receive traffic.

GUI Elements	Description
Type (continued)	If you choose a Minimum, Average, or Maximum Capacity report, the tables and graphs show capacity statistics for the backhaul interface. You can choose from 15-minute, hourly, or daily capacity reports. If Output Type is Graph, send and receive rate statistics appear in separate panes. Each pane shows two fully expandable graphs: • Top—Shows total (GSM-Abis and UMTS-Iub), total GSM-Abis, and total UMTS-Iub traffic rates, including percentage of backhaul utilization (right side of graph). • Bottom—Shows traffic rates for each shorthaul interface that belongs to the backhaul.
Table	Note Different tables appear depending on the report Type and Output Type selections. If the Output Type is Graph, a table appears with these columns: • Data Type—Type of data, send or received • Average—Average of the data across the chosen time range • Minimum—Minimum value across the chosen time range • Minimum Timestamp EDT—Time the minimum value occurred • Maximum—Maximum value across the chosen time range • Maximum Timestamp EDT—Time the maximum value occurred Note If the Output Type is Table or CSV, similar data is presented but the column headings may vary. Also, if the value is N/A, that means no data is available. Another table has these columns: • Data Type—Category of error for which statistics are gathered. Types include optimization, missed packets, and miscellaneous errors. • Total Counts—Total error count for each type of error. • Avg. Error Rate (Per Sec)—The calculated average error rate per second for each error type over the duration of the data range that you chose. Note You can sort the contents of the columns in ascending or descending order by clicking the column heading.
Expand to Full Screen	If Output Type is Graph, text link that shows a graph in a new, full-screen window for easier viewing.
Bits/Sec	If Output Type is Graph, primary Y-axis label (left side of graph) that shows traffic rate in bits per second. The Y axis automatically scales to the User Bandwidth. See the “Editing Properties for a RAN-O Backhaul” section on page 6-36. Note If no data exists between any two data points, the graph displays a color-coded vertical bar to show the period for which no data is available.

GUI Elements	Description
% Utilization	If Output Type is Graph, secondary Y-axis label (right side of graph) that shows the backhaul utilization as a percentage of the User Bandwidth. The graph background has three horizontal bars that are color-coded to indicate these thresholds: - Overloaded—Top portion of graph. - Warning—Middle portion of graph. - Acceptable—Bottom portion of graph. For definitions of these thresholds, see the “Threshold Information (RAN-O Only)” section on page 8-43. To change the threshold settings, see the “Editing Properties for a RAN-O Backhaul” section on page 6-36. Note If the % Utilization exceeds 100%, see Why does my backhaul utilization graph show greater than 100% for transmit traffic?, page C-22.
Time	X-axis label that shows a user-specified, historical time scale and the server time zone.
Legend	Color-coded legend that shows labels for traffic and error rates.

Displaying Error Statistics

You can view error data for a shorthaul or backhaul interface in the MWTM:

- Web interface by selecting an interface in the navigation tree and clicking the Shorthaul Errors or Errors tab in the content area.
- Client by right-clicking an interface in the navigation tree and clicking **Error History**.



Note

If the CISCO-IP-RAN-BACKHAUL-MIB on the node is not compliant with the MWTM, the MWTM issues the message:

```
MIB not compliant for reports
```

Install a version of IOS software on the node that is compatible with the MWTM. For a list of compatible IOS software, from the MWTM:

- Web interface, choose **Administrative > IPRAN OS README**.
- Client interface, choose **View > Web > Administrative**; then click **IPRAN OS README**.

You view error data for a shorthaul or backhaul interface by selecting the interface in the navigation tree and clicking the Errors tab in the content area. The Errors tab shows total error counts and average error rates in table and graph format.

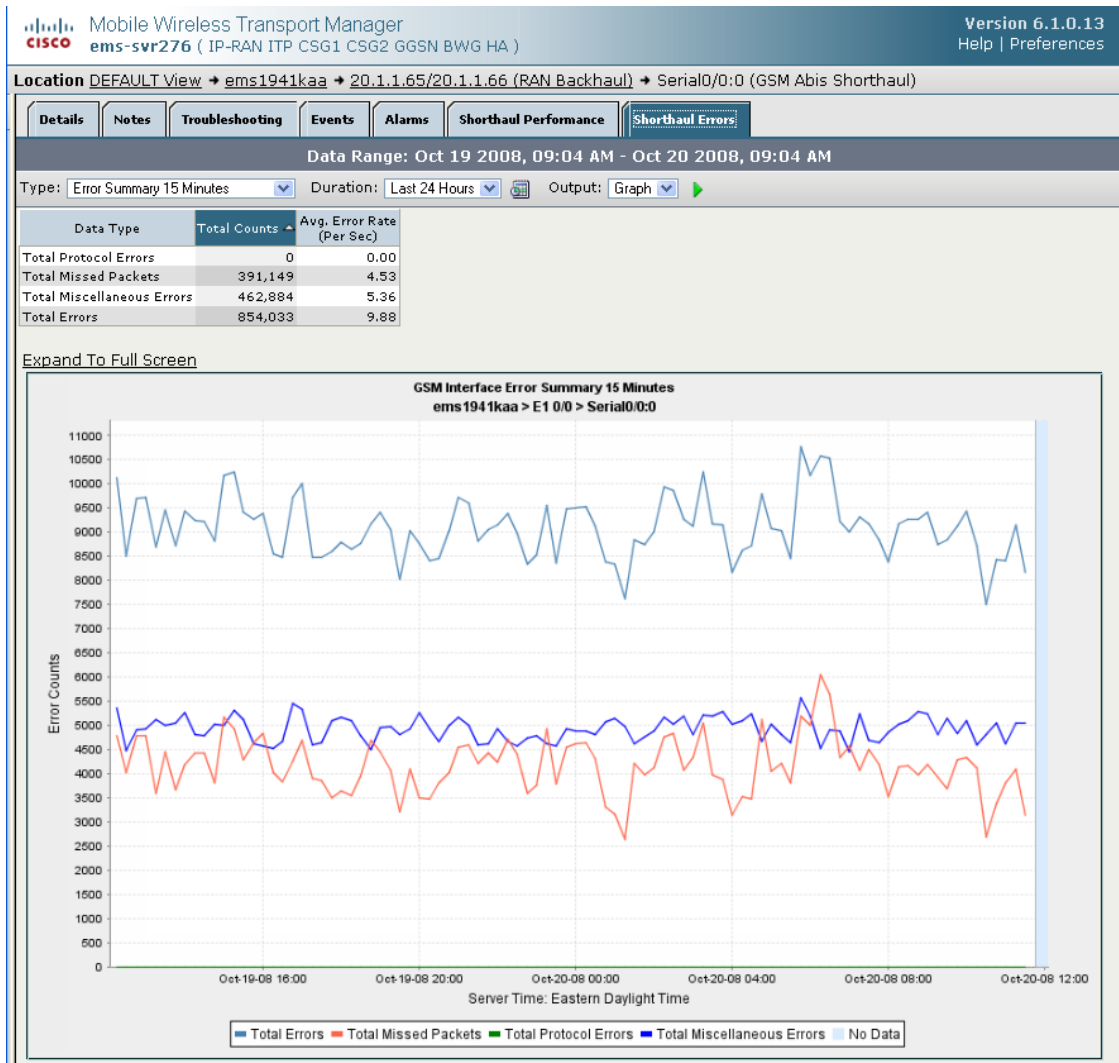
This section provides information about:

- [Displaying Shorthaul Error Statistics, page 11-40](#)
- [Displaying Backhaul Error Statistics, page 11-42](#)

Displaying Shorthaul Error Statistics

The Shorthaul Errors tab for a shorthaul interface shows a single table and a graph that shows the error rates and counts for different types of GSM-Abis and UMTS-Iub errors.

Figure 11-4 Example of Errors Tab for Shorthaul Interface



251018

The Shorthaul Errors tab for a shorthaul interface contains:

GUI Elements	Description
<i>Toolbar</i>	Provides functions to select report type, duration, and output type. See the “Using the Toolbar” section on page 11-5 .
Type	Report Type. If you choose an Error Summary report, the table and graph display a comprehensive summary of total error counts and average error rates for protocol, missed-packet, and miscellaneous errors for the chosen shorthaul. You can choose from 15-minute, hourly, or daily error summary reports. Statistics appear in table and graph format.
Type (continued)	If you choose an error report that is not a summary report, the table and graph displays protocol, missed packet, or miscellaneous errors for the shorthaul interface. You can choose from 15-minute, hourly, or daily error reports. Statistics appear in table and graph format. For definitions of these error types, see: • Protocol Failures, page 8-117 • Miscellaneous, page 8-118 • Missed Packets, page 8-119
<i>Table</i>	Note Different tables and column headings appear depending on the report Type and Output Type selections. If Output Type is Graph, a table appears with these columns: • Data Type—Category of error for which statistics are gathered. Types include protocol, missed packets, and miscellaneous errors. • Total Counts—Total error count for each type of error. • Avg. Error Rate (Per Sec)—The calculated average error rate per second for each error type over the duration of the data range that you chose. Note If the value is N/A, that means no data is available. Depending on the report Type selection, if the Output Type is Table or CSV, a table appears with multiple columns showing various error types and their counts. For definitions of these error types, see the: • Protocol Failures, page 8-117 • Miscellaneous, page 8-118 • Missed Packets, page 8-119 Note You can sort the contents of the columns in ascending or descending order by clicking the column heading.
Expand to Full Screen	If Output Type is Graph, this text link displays a graph in a new, full-screen window for easier viewing.
Error Counts	If Output Type is Graph, Y-axis label on left side of graph that shows traffic rate in bits per second. Note If no data exists between any two data points, the graph displays a color-coded vertical bar to show the period for which no data is available.

GUI Elements	Description
Time	If Output Type is Graph, X-axis label that shows a user-specified, historical time scale and the server time zone.
Legend	If Output Type is Graph, color-coded legend that shows labels for traffic and error rates.

Displaying Backhaul Error Statistics

The Errors tab for a RAN backhaul interface shows a single table and a graph that shows the error rates and counts for different interfaces belonging to the backhaul.

Figure 11-5 Example of Errors Tab for Backhaul Interface



251019

The Errors tab for a backhaul interface contains:

GUI Elements	Description
<i>Toolbar</i>	Provides functions to select a report type, duration, output type, and the Graph Series Editor. See the “Using the Toolbar” section on page 11-5.
<i>Table</i>	Note Different tables and column headings appear depending on the report Type and Output Type selections. If Output Type is Graph, a table appears with these columns: • Data Type—Category of error for which statistics are gathered. Types include optimization, missed packets, and miscellaneous errors. • Total Counts—Total error count for each type of error. • Avg. Error Rate (Per Sec)—The calculated average error rate per second for each error type over the duration of the data range that you chose. Note If the value is N/A, that means no data is available. If Output Type is Table, a table appears with columns for total error counts for various error types (for example, total GSM-Abis errors). Note You can sort the contents of the columns in ascending or descending order by clicking the column heading.
<i>Expand to Full Screen</i>	If Output Type is Graph, text link that shows a graph in a new, full-screen window for easier viewing.
<i>Error Counts</i>	If Output Type is Graph, Y-axis label on left side of graph that shows traffic rate in bits per second.
<i>Time</i>	If Output Type is Graph, X-axis label that shows a user-specified, historical time scale and the server time zone.
<i>Legend</i>	If Output Type is Graph, color-coded legend that shows labels for traffic and error rates (for example, Total Errors UMTS-Iub).

Generating RAN Data Export Files

You can easily generate historical reports for RAN backhauls and shorthauls in the web interface. You can then export this data to a report with comma-separated values (CSV file). You can save this file to disk or open it with an application that you choose (for example, Microsoft Excel).

To export RAN data:

- Step 1** Select a RAN backhaul or shorthaul in the navigation tree of the web interface.
- Step 2** Click the Performance or Errors tab in the right pane.
- Step 3** Generate a report.
- Step 4** Click the Export the report as a CSV file icon .

Displaying CSG2 Real-Time Statistics

The MWTM enables you to display real-time statistics for CSG2 nodes in the MWTM web interface. To display real-time statistics, select the node in the navigation tree and click the Statistics tab. Four categories of statistics appear:

- [Global Statistics, page 11-44](#)
- [Load Statistics, page 11-45](#)
- [BMA Statistics, page 11-47](#)
- [Quota Server Statistics, page 11-48](#)
- [User Database Statistics, page 11-49](#)

**Note**

For toolbar details, see [Using the Toolbar, page 11-5](#).

Global Statistics

The Global Statistics pane contains:

Field	Description
User Current	The total number of users with one or more active sessions on the system.
Session Current	The total number of sessions on the system. A session corresponds to a transmission control protocol (TCP) or user datagram protocol (UDP) flow.
User High Water	The highest number of active users reported by the User Current field since its last reset.
Session High Water	The highest number of active sessions reported by the Session Current field since its last reset.
<i>The following statistics are available only on CSG2, Release 2, for devices running IOS 12.4(15) or later.</i>	
GTP BMA Rejected	Number of messages received from all the BMAs with reject cause code.
GTP BMA Dropped	Total Number of messages dropped destined for any of the BMAs
GTP BMA Retransmit	The number of messages retransmitted to all BMAs.
GTP QuotaMgr Dropped	Number of messages received from all the Quota Managers with reject cause code.
GTP QuotaMgr Dropped	Total Number of messages dropped destined for any of the Quota Managers.
GTP QuotaMgr Retransmit	The number of messages retransmitted to all the Quota Managers.

Load Statistics

Load statistics are available only on CSG2, Release 2, for devices running IOS 12.4(15) or later.

The Load Statistics pane contains:

		Description
Statistics Type	Column	Defines the type of statistics for each row: - Radius Start Requests - Session Create Requests - BMA Messages - Messages to Quota Server - User Database Requests
Radius Start Requests	Allowed	Number of outgoing Radius Start requests allowed.
	Allowed Rate	Number of outgoing Radius Start requests allowed per second.
	Allowed Rate High Water	The highest number of outgoing Radius Start requests allowed per second.
	IPC Queue Depth Tolerance	Maximum queue depth for Radius Start requests in the IPC queue.
	Denied	Number of outgoing Radius Start requests denied.
	Denial Rate	Number of outgoing Radius Start requests denied per second.
	Denial Rate High Water	The highest number of outgoing Radius Start requests denied per second.
Session Create Requests	Allowed	Number of outgoing Session Create Requests allowed.
	Allowed Rate	Number of outgoing Session Create Requests allowed per per second.
	Allowed Rate High Water	The highest number of outgoing Session Create Requests allowed per second.
	IPC Queue Depth Tolerance	Maximum queue depth for Session Create Requests in the IPC queue.
	Denied	Number of outgoing Session Create Requests denied.
	Denial Rate	Number of outgoing Session Create Requests denied per second.
	Denial Rate High Water	The highest number of outgoing Session Create Requests denied per second.

		Description
BMA Messages	Allowed	Number of outgoing BMA messages allowed.
	Allowed Rate	Number of outgoing BMA messages allowed per second.
	Allowed Rate High Water	The highest number of outgoing BMA messages allowed per second.
	IPC Queue Depth Tolerance	Maximum queue depth for BMA messages in the IPC queue.
	Denied	Number of outgoing BMA messages denied.
	Denial Rate	Number of outgoing BMA messages denied per second.
	Denial Rate High Water	The highest number of outgoing BMA messages denied per second.
Messages to Quota Server	Allowed	Number of outgoing messages to Quota Manager allowed.
	Allowed Rate	Number of outgoing messages to Quota Manager allowed per second.
	Allowed Rate High Water	The highest number of outgoing messages to Quota Manager allowed per second.
	IPC Queue Depth Tolerance	Maximum queue depth for messages to Quota Manager in the IPC queue.
	Denied	Number of outgoing messages to Quota Manager denied.
	Denial Rate	Number of outgoing messages to Quota Manager denied per second.
	Denial Rate High Water	The highest number of outgoing messages to Quota Manager denied per second.
User Database Requests	Allowed	Number of outgoing User Database requests allowed.
	Allowed Rate	Number of outgoing User Database requests allowed per second.
	Allowed Rate High Water	The highest number of outgoing User Database requests allowed per second.
	IPC Queue Depth Tolerance	Maximum queue depth for User Database requests in the IPC queue.
	Denied	Number of outgoing User Database requests denied.
	Denial Rate	Number of outgoing User Database requests denied per second.
	Denial Rate High Water	The highest number of outgoing User Database requests denied per second.

BMA Statistics

The Billing Mediation Agent (BMA) Statistics pane contains:

Column	Description
Server	Name of the BMA server.
Port	The UDP port of the BMA.
VRF Name	Name of the virtual routing and forwarding (VRF) over which communication with BMA occurs. If no VRF is specified, the global routing table is used.
State	The state of the BMA. Possible states include: - Standby—The server is prepared to become active. - Failed—The server has failed to respond to requests. - Active—The server has been activated to receive requests. - Echowait—An echo request to this billing mediation agent is waiting for a response. - Nawait—A node-alive request to this billing mediation agent is waiting for a response. - Suspended—The server has received a stop request from the operator.
Lost Records	Total number of lost records since system initialization or the last time the counter wrapped.
Total Sent	Total number of records sent to the billing mediation agent.
Failed Acks	Number of acknowledgments received from the billing mediation agent for which there are no outstanding requests.
Outstanding	Current number of messages waiting to be acknowledged. An arrow icon indicates the trend (up or down) since the last poll.
Outstanding High Water	The highest number of messages waiting for acknowledgements as reported by the Outstanding field since its last reset.
Bad Records	The number of bad records received. These are records in which an error was detected while attempting to decode the contents.
Retransmits	The number of messages retransmitted to the billing mediation agent.
Sent Rate	Rate at which records are sent to the billing mediation agent.
<i>The following statistics are available only on CSG2, Release 2, for devices running IOS 12.4(15) or later.</i>	
Rate Interval	The duration of time interval in Packet Rate and Ack Rate.
Packet Rate	Number of packets sent to the BMA per second calculated over the interval indicated by Rate Interval.
Ack Rate	Number of acknowledgments received from the BMA per second calculated over the interval indicated by Rate Interval.

Quota Server Statistics

The Quota Server Statistics pane contains:

Column	Description
Server	Name of the quota server.
Port	The UDP port of the quota server.
VRF Name	Name of the VRF over which communication with the quota server occurs. If no VRF is specified, the global routing table is used.
State	The state of the quota manager. Possible states include: - Standby—The quota manager is prepared to become active. - Failed—The quota manager has failed to respond to requests. - Active—The quota manager has been activated to receive requests. - Echowait—An echo request to this quota manager is waiting for a response. - Nawait—A node-alive request to this quota manager is waiting for a response. - Suspended—The quota manager has received a stop request from the operator.
Lost Records	Total number of lost records since system initialization or the last time the counter wrapped.
Total Sent	Total number of records sent to the quota server.
Failed Acks	Number of acknowledgments received from the quota server for which there are no outstanding requests.
Outstanding	Current number of messages waiting to be acknowledged. An arrow icon indicates the trend (up or down) since the last poll.
Outstanding High Water	The highest number of messages waiting for acknowledgements as reported by the Outstanding field since its last reset.
Bad Records	The number of bad records received. These are records in which an error was detected while attempting to decode the contents.
Retransmits	The number of messages retransmitted to the quota manager.
Sent Rate	Rate at which records are sent to the quota server.
<i>The following statistics are available only on CSG2, Release 2, for devices running IOS 12.4(15) or later.</i>	
Rate Interval	The duration of time interval in Packet Rate and Ack Rate.
Packet Rate	Number of packets sent to the Quota Manager per second calculated over the interval indicated by Rate Interval.
Ack Rate	Number of acknowledgments received from the Quota Manager per second calculated over the interval indicated by Rate Interval.

User Database Statistics

The user database is a service that translates a client IP address into a user identifier. The User Database Statistics pane contains:

Column	Description
Server	Name of the user database server.
Port	The listening UDP port of the server.
VRF Name	Name of the VRF over which communication with user data server occurs. If no VRF is specified, the global routing table is used.
State	State of the user database. Possible values include: Reset—State before the database is determined to be active. Active—The database is available and processing requests. Failed—The database has failed and is not processing requests.
Requests	Number of user database requests.
User Identifiers Returned	Number of user identifiers returned.
Requests Resent	Number of user database requests resent.
Request Timeouts	Number of user database requests that have timed out.
Request Errors	Number of errors returned on user database requests.
Requests Rate	Rate of user database requests.
User Identifiers Returned Rate	Rate at which user identifiers are returned.

Displaying BWG Real-Time Statistics

The MWTM enables you to display real-time statistics for Broadband Wireless Gateway (BWG) nodes in the MWTM web interface. To display BWG real-time statistics, select a BWG node in the navigation tree and click the Statistics tab. These four subtabs appear:

- [Global Statistics, page 11-49](#)
- [Paths Statistics, page 11-58](#)
- [User Groups Statistics, page 11-59](#)

Global Statistics

The Global statistics subtab shows global statistics for BWG nodes and contains:

- [Status, page 11-50](#)
- [Creation and Deletion Statistics, page 11-51](#)
- [Miscellaneous Statistics, page 11-52](#)
- [Signaling Packet Statistics, page 11-53](#)

- [DHCP Packet Statistics, page 11-53](#)
- [Handoff Statistics, page 11-54](#)
- [Data Packet Statistics, page 11-55](#)
- [Dropped Packet Statistics, page 11-56](#)
- [Profile Statistics, page 11-57](#)
- [Rejected Statistics, page 11-58](#)

**Note**

For toolbar details, see [Using the Toolbar, page 11-5](#).

Status

The Status pane shows:

Field	Description
Version	Software version of the BWG.
Description	Description of the physical instance of the BWG.
Operational State	Current operational state of the BWG.
Session Redundancy Status	Indicates whether session redundancy is enabled or disabled.

Creation and Deletion Statistics

The Creation and Deletion Statistics pane shows:

Field	Description
Base Stations	• Maximum—Maximum number of base stations that can be concurrently supported by this BWG. • Current—Current number of signaling paths to all base stations. One signaling path is created between the BWG and each base station, so the current number of signaling paths is equal to the number of base stations currently connected to the BWG. • Created Count—Total number of signaling paths created on this BWG which include active and past signaling paths. • Created Rate—Rate at which signaling paths are created. • Deleted Count—Total number of signaling paths deleted on this BWG. • Deleted Rate—Rate at which signaling paths are deleted.
Data Paths	• Maximum—N/A • Current—Current number of data paths to all base stations. • Created Count—Total number of data paths created on this BWG which include active and past data paths. • Created Rate—Rate at which data paths are created. • Deleted Count—Total number of data paths deleted on this BWG. • Deleted Rate—Rate at which data paths are deleted.
Subscribers	• Maximum—Maximum number of subscribers that can be concurrently supported by this BWG. • Current—Number of subscribers currently connected to this BWG. • Created Count—Total number of subscribers created on this BWG which includes active and past subscribers • Created Rate—Rate at which subscribers are created. • Deleted Count—Total number of subscribers deleted on this BWG. • Deleted Rate—Rate at which subscribers are deleted.
Sessions	• Maximum—N/A • Current—Number of sessions currently active on this BWG. • Created Count—Total number of sessions created on this BWG which include active and past sessions. • Created Rate—Rate at which sessions are created. • Deleted Count—Total number of sessions deleted on this BWG. • Deleted Rate—Rate at which sessions are deleted.

Field	Description
Flows	• Maximum—N/A • Current—Current number of flows for all sessions active on this BWG. • Created Count—Total number of flows created on this BWG which include active and past flows. • Created Rate—Rate at which flows are created. • Deleted Count—Total number of flows deleted on this BWG. • Deleted Rate—Rate at which flows are deleted.
Hosts	• Maximum—N/A • Current—Current number of hosts connected to this BWG. • Created Count—Total number of hosts created on this BWG which include active and past hosts. • Created Rate—Rate at which hosts are created. • Deleted Count—Total number of hosts deleted on this BWG. • Deleted Rate—Rate at which hosts are deleted.

Miscellaneous Statistics

The Miscellaneous Statistics pane shows:

Field	Description
Framed Routes	Indicates the current number of unique framed routes downloaded from AAA and inserted into the IP routing table on a gateway.
Framed Router Subscribers	Indicates the number of subscribers using framed routes.
Auto-Provisioned Sessions	Indicates the number of auto-provisioned sessions on gateway.
Redirected Sessions	Indicates the number of sessions with all uplink IP packets redirected by the gateway.
Networks behind Mobile Stations	Indicates the number of networks behind mobile stations.
Aged Out Hosts	Count—Indicates the number of idle static hosts aged out. Rate—Rate at which idle static hosts are aged out.

Signaling Packet Statistics

The Signaling Packet Statistics pane shows:

Field	Description
Pending	Count—Total number of signaling packets currently pending on this BWG
Processed	- Count—Total number of signaling packets processed by this BWG. - Rate—Rate at which signaling packets are processed.
Requeued	- Count—Total number of signaling packets that were requeued on this BWG. - Rate—Rate at which signaling packets are requeued.
Congestion Drops	- Count—Number of signaling packets dropped when too many signaling packets are queued. The current queue limit is 1000 packets. - Rate—Rate at which signaling packets are dropped.
Service Disabled Drops	- Count—Number of signaling packets dropped due to disabled service. - Rate—Rate at which signaling packets are dropped.
Service Not Ready Drops	- Count—Number of signaling packets dropped while in non-active state for redundant configuration. - Rate—Rate at which signaling packets are dropped.
Encapsulation Errors Drops	- Count—Number of signaling packets dropped due to encapsulation errors. - Rate—Rate at which signaling packets are dropped.
Disposed Drops	- Count—Number of signaling packets disposed by the BWG. - Rate—Rate at which signaling packets are disposed.

DHCP Packet Statistics

The DHCP Packet Statistics pane shows:

Field	Description
Discover	- Count—Number of DHCP discover packets. - Rate—Rate at which DHCP packets are discovered.
Offer	- Count—Number of DHCP offer packets. - Rate—Rate at which DHCP packets are offered.
Request	- Count—Number of DHCP request packets. - Rate—Rate at which DHCP packets are requested.
Decline	- Count—Number of DHCP decline packets. - Rate—Rate at which DHCP packets are declined.
Ack	- Count—Number of DHCP acknowledged packets. - Rate—Rate at which DHCP packets are acknowledged.
Nak	- Count—Number of DHCP negatively acknowledged packets. - Rate—Rate at which DHCP packets are negatively acknowledged.

Field	Description
Release	- Count—Number of DHCP release packets. - Rate—Rate at which DHCP packets are released.
Inform	- Count—Number of DHCP inform packets. - Rate—Rate at which DHCP packets are informed.
Lease Query	- Count—Number of DHCP lease query packets. - Rate—Rate at which DHCP packets are lease queried.
Unknown	- Count—Number of DHCP unknown packets. - Rate—Rate at which DHCP packets are unknown.

Handoff Statistics

The Handoff Statistics pane shows:

Field	Description
Successful Handoffs	- Count—Number of successful session handoffs between Base Stations. - Rate—Rate at which successful session handoffs occur.
Failed Handoffs	- Count—Number of failed session handoffs between Base Stations. - Rate—Rate at which failed session handoffs occur.
Successful CMAC Key Updates	- Count—Number of successful CMAC Key count updates related to handoff between base stations. - Rate—Rate at which successful CMAC Key count updates are received.
Failed CMAC Key Updates	- Count—Number of failed CMAC Key count updates related to handoff between base stations. - Rate—Rate at which failed CMAC Key count updates are received.
Successful Security Key Exchanges	- Count—Number of successful security key exchanges during handoff between base stations. - Rate—Rate at which successful security key exchanges occur.
Failed Security Key Exchanges	- Count—Number of failed security key exchanges during handoff between base stations. - Rate—Rate at which failed security key exchanges occur.

Data Packet Statistics

The Data Packet Statistics pane shows:

Field	Description
Received IP Packets	- Count—Number of data packets received by the BWG. - Rate—Rate at which data packets are received by the BWG.
Received IP Bytes	- Count—Number of data bytes received by the BWG. - Rate—Rate at which data bytes are received by the BWG.
Sent IP Packets	- Count—Number of data packets sent by the BWG. - Rate—Rate at which data packets are sent by the BWG.
Sent IP Bytes	- Count—Number of data bytes sent by the BWG. - Rate—Rate at which data bytes are sent by the BWG.
Redirected IP Packets	- Count—Number of IP packets redirected by the BWG. - Rate—Rate at which IP packets are redirected by the BWG.
Redirected IP Bytes	- Count—Number of IP bytes redirected by the BWG. - Rate—Rate at which IP bytes are redirected by the BWG.
Received Ethernet Packets	- Count—Number of ethernet packets received by the BWG. - Rate—Rate at which IP packets are redirected by the BWG.
Received Ethernet Bytes	- Count—Number of ethernet packets received by the BWG. - Rate—Rate at which ethernet packets are received by the BWG.
Sent Ethernet Packets	- Count—Number of ethernet packets sent by the BWG. - Rate—Rate at which ethernet packets are sent by the BWG.
Sent Ethernet Bytes	- Count—Number of ethernet bytes sent by the BWG. - Rate—Rate at which ethernet bytes are sent by the BWG.
Redirected Ethernet Packets	- Count—Number of ethernet packets redirected by the BWG. - Rate—Rate at which ethernet packets are redirected by the BWG.
Redirected Ethernet Bytes	- Count—Number of ethernet bytes redirected by the BWG. - Rate—Rate at which ethernet bytes are redirected by the BWG.
Punted Data Packets	- Count—Number data packets punted from the cef path to the process path. - Rate—Rate at which packets are punted from the cef path to the process path.

Dropped Packet Statistics

The Dropped Packet Statistics pane shows:

Field	Description
Encapsulation Errors Drops	- Count—Number of data packets dropped due to encapsulation errors. - Rate—Rate at which data packets are dropped.
Invalid Address Drops	- Count—Number of data packets dropped due to invalid IP address. - Rate—Rate at which data packets are dropped.
Service Disabled Drops	- Count—Number of data packets dropped due to disabled service. - Rate—Rate at which data packets are dropped.
Invalid Protocol Type Drops	- Count—Number of data packets dropped due to invalid protocol types. - Rate—Rate at which data packets are dropped.
Length Error Drops	- Count—Number of data packets dropped due to IP packet length errors. - Rate—Rate at which data packets are dropped.
Absent Key Drops	- Count—Number of data packets dropped due to GRE key errors. - Rate—Rate at which data packets are dropped.
Flow Not Found Drops	- Count—Number of data packets dropped due to flow not found errors. - Rate—Rate at which data packets are dropped.
Flow Path Not Found Drops	- Count—Number of data packets dropped due to flow path not found errors. - Rate—Rate at which data packets are dropped due to flow path not found errors.
Flow Path Invalid Source Drops	- Count—Number of data packets dropped due to invalid source path address errors in the GRE header. - Rate—Rate at which data packets are dropped due to invalid source path address errors in the GRE header.
Session Not Found Drops	- Count—Number of data packets dropped due to session not found errors for the GRE key. - Rate—Rate at which data packets are dropped due to session not found errors.
Subscriber Not Found Drops	- Count—Number of data packets dropped due to subscriber not found errors for the GRE key. - Rate—Rate at which data packets are dropped due to subscriber not found errors.
Checksum Error Drops	- Count—Number of data packets dropped due to checksum errors. - Rate—Rate at which data packets are dropped due to checksum errors.
Ingress Filtering Drops	- Count—Number of data packets dropped due to subscriber invalid source IP address errors. - Rate—Rate at which data packets are dropped due to invalid source IP address errors.

Field	Description
Sequence Number Error Drops	- Count—Number of data packets dropped due to sequence number errors. - Rate—Rate at which data packets are dropped due to sequence number errors.
Fragmented Drops	- Count—Number of data packets dropped due to fragmented packet errors. - Rate—Rate at which data packets dropped due to fragmented packet errors.
Static IP Host Creation Failure Drops	- Count—Number of packets, such as upstream ARP and upstream data packets, dropped due to failure in creation of Static IP Host. - Rate—Rate at which data packets are dropped due to failure in creation of Static IP Host.
L2 Multicast and Broadcast Drops	- Count—Number of L2 multicast and broadcast data packets other than ARP and DHCP dropped by BWG. - Rate—Rate at which L2 multicast and broadcast data packets are dropped.
Throttled Path Punt Drops	- Count—Number of data packets dropped due to throttling of punts. - Rate—Rate at which L2 multicast and broadcast data packets are dropped.
Learned Static Hosts Drops	- Count—Number of data packets dropped due to BWG learning about static hosts from upstream data packets. - Rate—Rate at which data packets are dropped due to BWG learning about static hosts from upstream data packets.

Profile Statistics

The Profile Statistics pane shows:

Field	Description
Service Flow Profile Not Found	- Count—Number of service flow creation errors due to an unconfigured service flow profile. - Rate—Rate at which creation errors are received.
QoS Profile Not Found	- Count—Number of service flow creation errors due to an unconfigured service flow QoS profile. - Rate—Rate at which creation errors are received.
Classifier Profile Not Found	- Count—Number of service flow creation errors due to an unconfigured service flow packet classifier profile. - Rate—Rate at which service flow creation errors occur due to an unconfigured service flow packet classifier profile.
SLA Profile Not Found	- Count—Number number of session creation failures due to configuration error in Service Level Agreement (SLA) profile on BWG. - Rate—Rate at which session creation failures occur due to configuration error in Service Level Agreement (SLA) profile on BWG.

Rejected Statistics

The Rejected Statistics pane shows:

Field	Description
Rejected Base Station Paths	- Count—Number of paths rejected because they exceeded the maximum number of base stations allowed to connect to this BWG. - Rate—Rate at which paths are rejected because they exceeded the maximum number of base stations allowed to connect to this BWG.
Unapproved Base Station Sessions	- Count—Number of session creation and/or session handoffs rejected because the requesting base station is not approved for it. - Rate—Rate at which created sessions and/or session handoffs are rejected because the base station is not approved for it.
Rejected Subscriber Sessions	- Count—Number of sessions that were rejected due to exceeding the maximum number of allowed subscribers. - Rate—Rate at which sessions that were rejected due to exceeding the maximum number of allowed subscribers.
Rejected Session Flows	- Count—Number of flows that were rejected due to exceeding the maximum number of flows allowed per session. - Rate—Rate at which flows were rejected due to exceeding the maximum number of flows allowed per session.
Session Deleted by the Gateway	- Count—Number of sessions deleted by the BWG. - Rate—Rate at which sessions were deleted by the BWG.
Rejected Hosts Open Requests	- Count—Number of <i>hosts open</i> requests rejected. - Rate—Rate at which <i>hosts open</i> requests are rejected.

Paths Statistics



Note

For toolbar details, see [Using the Toolbar, page 11-5](#).

The Paths statistics subtab shows information and statistics about each base station and contains:

Column	Description
Remote IP Address	Path IP address at the base station side.
Local IP Address	Path IP address at the BWG side.
Type	Path type, can be signaling or data.
Sessions	Number of sessions over the path.
Flows	Number of flows over the path.
Sent IP Packets Count	Total number of IP packets sent over the path.

Column	Description
Sent IP Packets Rate	Rate at which IP packets are sent.
Sent IP Bits Count	Total number of IP bits sent over the path.
Sent IP Bits Rate	Rate at which IP bits are sent.
Received IP Packets Count	Total number of IP packets received over the path.
Received IP Packets Rate	Rate at which IP packets are received.
Received IP Bits Count	Total number of IP bits received over the path.
Received IP Bits Rate	Rate at which IP bits are received.
Sent Ethernet Packets Count	Total number of Ethernet packets sent over the path.
Sent Ethernet Packets Rate	Rate at which Ethernet packets are sent.
Sent Ethernet Bits Count	Total number of Ethernet bits sent over the path.
Sent Ethernet Bits Rate	Rate at which Ethernet bits are sent.
Received Ethernet Packets Count	Total number of Ethernet packets received over the path.
Received Ethernet Packets Rate	Rate at which Ethernet packets are received.
Received Ethernet Bits Count	Total number of Ethernet bits received over the path.
Received Ethernet Bits Rate	Rate at which Ethernet bits are received.

User Groups Statistics

The User Groups statistics subtab shows information and statistics for user groups and contains:

- [Sessions and Flow Statistics, page 11-60](#)
- [Traffic Statistics, page 11-60](#)



Note

For toolbar details, see [Using the Toolbar, page 11-5](#).

Sessions and Flow Statistics

The Sessions and Flow Statistics pane shows:

Column	Description
Name	Domain name identifying a user group.
Service Mode	User group service mode.
Current Session: Count	Total number of active sessions per user group.
Sessions Created: Count	Total number of sessions created per user group.
Sessions Created: Rate	Rate at which sessions are created.
Sessions Deleted: Count	Total number of sessions deleted per user group.
Sessions Deleted: Rate	Rate at which sessions are deleted.
Flows Created: Count	Total number of active flows per user group.
Flows Created: Rate	Rate at which flows are created.
Flows Deleted: Count	Total number of flows created per user group.
Flows Deleted: Rate	Rate at which flows are deleted.
Group Overwrites: Count	Number of times this user group has been overwritten by user group received from the AAA server. Users can belong to a particular user group at the time of initial entry and the AAA server can recategorize the user under a different user group after successful authentication.
Group Overwrites: Rate	Rate at which this user group has been overwritten by user group received from the AAA server.

Traffic Statistics

The Traffic Statistics pane shows:

Column	Description
Name	Domain name identifying a user group.
Service Mode	User group service mode.
Sent IP Packets Count	Total number of IP packets sent over the path.
Sent IP Packets Rate	Rate at which IP packets are sent.
Sent IP Bits Count	Total number of IP bits sent over the path.

Column	Description
Sent IP Bits Rate	Rate at which IP bits are sent.
Received IP Packets Count	Total number of IP packets received over the path.
Received IP Packets Rate	Rate at which IP packets are received.
Received IP Bits Count	Total number of IP bits received over the path.
Received IP Bits Rate	Rate at which IP bits are received.
Sent Ethernet Packets Count	Total number of Ethernet packets sent over the path.
Sent Ethernet Packets Rate	Rate at which Ethernet packets are sent.
Sent Ethernet Bits Count	Total number of Ethernet bits sent over the path.
Sent Ethernet Bits Rate	Rate at which Ethernet bits are sent.
Received Ethernet Packets Count	Total number of Ethernet packets received over the path.
Received Ethernet Packets Rate	Rate at which Ethernet packets are received.
Received Ethernet Bits Count	Total number of Ethernet bits received over the path.
Received Ethernet Bits Rate	Rate at which Ethernet bits are received.
Received: Packets Rate	Rate at which packets are received.
Received: Bits Count	Total number of bits received by this user group.
Received: Bits Rate	Rate at which bits are received.
Invalid Source Packets: Count	Number of packets dropped due to invalid source address errors.
Invalid Source Packets: Rate	Rate at which packets are dropped.
Invalid Source Bits: Count	Number of bits dropped due to invalid source address errors.
Invalid Source Bits: Rate	Rate at which bits are dropped.

Displaying HA Real-Time Statistics

The MWTM enables you to display real-time statistics for Home Agent (HA) nodes in the MWTM web interface. To display HA real-time statistics, select a HA node in the navigation tree and click the Statistics tab. These subtabs appear:

- [Global, page 11-62](#)
- [IP Local Pool Config, page 11-64](#)
- [IP Local Pool Stats, page 11-64](#)

Global

The Global subtab shows global statistics for HA nodes and contains:

- Registrations Processed by AAA
- Registration Requests
- Standby Synchronization



Note

For toolbar details, see [Using the Toolbar, page 11-5](#).

Registrations Processed by AAA

The Registrations Processed by AAA pane shows:

Field	Description
Maximum Processed in one minute	The maximum number of registration requests processed in a minute by the HA. It includes only those registration requests which were authenticated by the AAA server.
Average time to process (msecs)	The average time taken by the home agent to process a registration request. Calculations are based on only those registration requests that were authenticated by the AAA server.
Authenticated via AAA Server	• Count—The total number of registration requests processed by the home agent, including only those registration requests that were authenticated by the AAA server. • Rate—The total rate of registration requests processed by the home agent, including only those registration requests that were authenticated by the AAA server.

Registration Requests

The Registration Requests pane shows:

Field	Description
Current Bindings	- Count—The current number of entries in the home agent's mobility binding list. The home agent updates this number in response to registration events from mobile nodes. - Rate—The count can increment or decrease, resulting in a positive or negative rate.
Initial Received	- Count—Total number of initial registration requests received by the HA. - Rate—Rate at which initial registration requests are received by the HA.
Initial Denied	- Count—Total number of initial registration requests denied by the HA. - Rate—Rate at which initial registration requests are denied by the HA.
All Received	- Count—Total number of all registration requests received by the HA. - Rate—Rate at which all registration requests are received by the HA.
All Denied	- Count—Total number of all registration requests denied by the HA. - Rate—Rate at which all registration requests are denied by the HA.

Standby Synchronization

The Standby Synchronization pane shows:

Field	Description
Binding Updates Sent	- Count—Total number of binding updates sent by the home agent to a standby home agent. - Rate—Total rate of binding updates sent by the home agent to a standby home agent.
Binding Updates Unacknowledged	- Count—Total number of binding updates sent by the home agent for which no acknowledgement is received from the standby home agent. - Rate—Total rate of binding updates sent by the home agent for which no acknowledgement is received from the standby home agent.

IP Local Pool Config

**Note**

For toolbar details, see [Using the Toolbar, page 11-5](#).

The IP Local Pool Config subtab shows IP addresses for HA nodes and contains:

Column	Description
Name	Name that uniquely identifies an IP local pool. This name must be unique among all the local IP pools even when they belong to different pool groups.
Low	This object specifies the first IP address of the range of IP addresses contained by this pool entry. This address must be less than or equal to the High address.
High	This object specifies the last IP address of the range of IP addresses mapped by this pool entry. If only a single address is being mapped, the value of this object is equal to the Low value.
Free	The number of IP addresses available for use in the range of IP addresses.
In Use	The number of IP addresses being used in the range of IP addresses.
Priority	This object specifies the priority of the IP local pool. IP local pools will be used in assigning IP addresses in the order of priority.

IP Local Pool Stats

**Note**

For toolbar details, see [Using the Toolbar, page 11-5](#).

The IP Local Pool Stats subtab shows IP addresses and IP addresses in use for HA nodes and contains:

Column	Description
Name	Name that uniquely identifies an IP local pool. This name must be unique among all the local IP pools even when they belong to different pool groups.
Free	The number of IP addresses available for use in this IP local pool.
In Use	The number of IP addresses being used in this IP local pool.
Maximum In Use	Contains the high water mark of used addresses in an IP local pool since pool creation, since the system was restarted, or since this object was reset, whichever occurred last.
Low Threshold	When the number of used addresses in an IP local pool falls below this threshold value, a notification is generated.
High Threshold	When the number of used addresses in an IP local pool is equal or exceeds this threshold value, a notification is generated.
Low Threshold Percentage	When the percentage of used addresses in an IP local pool falls below this threshold value, a notification is generated.
High Threshold Percentage	When the percentage of used addresses in an IP local pool is equal or exceeds this threshold value, a notification is generated.

Displaying GGSN Real-Time Statistics

The MWTM enables you to display real-time statistics only in the MWTM web interface for Gateway GPRS Support Nodes (GGSNs) that reside on the Service and Application Module for IP (SAMI). To display GGSN real-time statistics, select a SAMI-based GGSN node in the navigation tree and click the Statistics tab. These subtabs appear:

- [Global, page 11-65](#)
- [SGSN Throughput, page 11-68](#)
- [APN General, page 11-69](#)
- [APN Throughput Statistics, page 11-70](#)
- [IP Local Pool Config, page 11-71](#)
- [IP Local Pool Stats, page 11-72](#)

Global

**Note**

For toolbar details, see [Using the Toolbar, page 11-5](#).

The Global subtab shows global statistics for GGSN nodes and contains:

- [GTP Statistics, page 11-65](#)
- [Charging Statistics, page 11-66](#)
- [GTP Throughput Statistics, page 11-66](#)
- [PDP Context Statistics, page 11-66](#)
- [AAA Statistics, page 11-68](#)
- [IP and UDP Statistics, page 11-68](#)

GTP Statistics

The GTP Statistics pane displays statistics about the GPRS Tunneling Protocol (GTP) and contains:

Column	Description
GTP Signaling Messages	GTP signaling messages sent between the Serving GPRS Support Node (SGSN) and GGSN.
G-PDU Messages	GTP Packet Data Unit (G-PDU) messages received on an SGSN path.
G-PDU Octets	Bytes sent and received in a GTP PDU message on an SGSN path.
Sent	Count—The number of messages or bytes in the transmit direction. Rate—The transmit rate of the messages or bytes.
Received	Count—The number of messages or bytes in the receive direction. Rate—The receive rate of the messages or bytes.

Charging Statistics

The Charging Statistics pane displays count and rate statistics for GGSN charging messages and contains:

Column	Description
G-CDR Messages Pending	GGSN Call Detail Records (CDRs) that are pending.
G-CDR Messages Sent	G-CDRs that were sent.

GTP Throughput Statistics

The GTP Throughput Statistics pane displays count and rate statistics about GTP throughput and contains:

Column	Description
GTP Packets	GTP packets between the GGSN and SGSN.
GTP Bytes	GTP bytes between the GGSN and SGSN.
Sampling Interval in Minutes: 3	Global GTP throughput statistics on the GGSN for a duration of 3 minutes.
Sampling Interval in Minutes: 5	Global GTP throughput statistics on the GGSN for a duration of 5 minutes.
Data age (minutes)	The difference in minutes between the time when the data was collected and retrieved. This is the time that has elapsed after the previous collection or update of the data.
Upstream	Rate (per second) of upstream GTP traffic during the last sampling period.
Downstream	Rate (per second) of downstream GTP traffic during the last sampling period.

PDP Context Statistics

The PDP Context Statistics pane shows count and rate values for these statistics:

Column	Description
Active GTP v0 PDP Contexts	PDP contexts (GTP version 0) that are active.
Active GTP v1 PDP Contexts	PDP contexts (GTP version 1) that are active.
PDP Contexts Created	PDP contexts that were created.
PDP Contexts Deleted	PDP contexts that were deleted.
PDP Activations Rejected	PDP contexts for which the activation request was rejected.

Column	Description
PDP Requests Dropped	Create PDP context requests and delete PDP context requests that were dropped because the threshold limit was reached for the maximum number of Point-to-point (PPP) regeneration sessions allowed on the GGSN.
PDP PPP-Regen Interfaces Created	Device-specific interfaces created for association with PDP contexts regenerated to a PPP session.
Active PDP Contexts with Direct Tunnel	Active PDP contexts with direct tunnel enabled.
PDP Contexts Deleted Without Waiting for the SGSN	PDPs deleted in the GGSN without waiting for a delete context response from the SGSN.
PDP Contexts Deleted Without Sending to the SGSN	PDPs deleted in the GGSN without sending a delete request to the SGSN.
Update PDP Context Requests Sent	Update PDP context requests that the GGSN initiated and that were sent to the SGSN.
Update PDP Context Responses Received	Update PDP context responses received from the SGSN for the GGSN-initiated update requests.
COA Messages Received	Change of Authorization (COA) messages received at the GGSN.
COA Messages Dropped	COA messages dropped at the GGSN.
COA QOS Updates Sent	Update PDP requests for QOS changes that COA initiated and that are sent from the GGSN.
Error Indication Messages Received	Error indication messages received on the GGSN.
Direct Tunnels Enabled	Direct tunnels enabled for the PDP contexts in the GGSN.
Error Indications for DT PDP Contexts	Error indications received for Direct Tunnel (DT) PDP contexts from the Radio Network Controller (RNC).
DT PDP Contexts Deleted Due to Update Response	Direct tunnel PDP contexts deleted because of update response failure.

AAA Statistics

The AAA Statistics pane shows:

Column	Description
AAA Server Name	Name of the Authentication, Authorization, and Accounting (AAA) server.
Server State	Whether the server is up (operational) or down (not operational).
Authentication Requests	Count and rate values for requests to the AAA server for authentication.
Accounting Requests	Count and rate values for requests to the AAA server for accounting services.

IP and UDP Statistics

The IP and UDP Statistics pane shows:

Column	Description
IP In Header Errors	Input datagrams discarded because of errors in their IP headers, including bad checksums, version number mismatches, other format errors, time-to-live exceeded, and errors discovered in processing their IP options.
IP Out Discards	Outbound packets that were discarded although no errors were detected. One reason for discarding a packet would be to free buffer space.
IP Out No Routes	IP datagrams discarded because no route could be found to transmit them. This statistic includes any datagrams that a host cannot route because all its default gateways are down.
IP Reassembly Fails	Failures detected by the IP reassembly algorithm.
IP Routing Discards	Routing entries that were discarded even though they are valid. One reason for discarding a routing entry would be to free buffer space for other routing entries.
UDP In Datagrams	UDP datagrams delivered to UDP users.

SGSN Throughput

**Note**

For toolbar details, see [Using the Toolbar, page 11-5](#).

The SGSN Throughput subtab shows:

Column	Description
SGSN Name	Name of the SGSN.
Sampling Interval in Minutes: 3	Throughput statistics on the SGSN for a duration of 3 minutes.

Column	Description
Sampling Interval in Minutes: 5	Throughput statistics on the SGSN for a duration of 5 minutes.
Upstream Packets	Rate (per second) of upstream packets sent on this SGSN during the last sampling period.
Upstream Bytes	Rate (per second) of upstream bytes sent on this SGSN during the last sampling period.
Downstream Packets	Rate (per second) of downstream packets sent on this SGSN during the last sampling period.
Downstream Bytes	Rate (per second) of downstream bytes sent on this SGSN during the last sampling period.
Data age (minutes)	The difference in minutes between the time when the data was collected and retrieved. This is the time that has elapsed after the previous collection or update of the data.

APN General



Note

For toolbar details, see [Using the Toolbar, page 11-5](#).

The APN General subtab contains:

- [APN Miscellaneous Statistics, page 11-69](#)
- [APN PDP Context Statistics, page 11-70](#)
- [APN Throughput Statistics, page 11-70](#)

APN Miscellaneous Statistics

To view the APN Miscellaneous Statistics table, choose this option from the Type drop-down menu. The GUI displays count and rate values for these statistics:

Column	Description
APN Name	The name of the Access Point Name (APN).
APN Index	A unique numerical identifier for the APN.
Upstream Payload Volume	The total payload volume in upstream traffic.
Downstream Payload Volume	The total payload volume in downstream traffic.
Source Address Violations	Upstream Transport PDUs (T-PDUs) that have been dropped because of source address violations.
COA Messages Received	COA messages received on this APN.

Column	Description
COA Messages Acknowledged	COA messages that were acknowledged by the GGSN with a COA ACK.
Direct Tunnels Enabled	Direct tunnels enabled for the PDP contexts on this APN.

APN PDP Context Statistics

To view the APN PDP Context Statistics table, choose this option from the Type drop-down menu. The GUI displays the count and rate values for these statistics:

Column	Description
APN Name	The name of the Access Point Name (APN).
APN Index	A unique numerical identifier for the APN.
PDP Activations Initiated by MS	PDP context activation procedures initiated by any mobile station (MS) on this APN.
PDP Activations Completed by MS	Successfully completed PDP context activation procedures initiated by MS on this APN.
PDP Deactivations Initiated by MS	PDP context deactivation procedures initiated by the MS on this APN.
PDP Deactivations Completed by MS	Successfully completed PDP context deactivation procedures initiated by the MS.
PDP Deactivations Initiated by GGSN	PDP context deactivation procedures initiated by the GGSN.
PDP Deactivations Completed by GGSN	Successfully completed PDP context deactivation procedures initiated by the GGSN.
Active PDP Contexts	Active PDP contexts in the APN.
Update PDP Context Requests Sent	GGSN-initiated update requests sent on this APN.
Update PDP Context Responses Received	Successful update responses received from the SGSN with a cause value of Request accepted for the GGSN-initiated update requests on this APN.

APN Throughput Statistics

To view the APN Throughput Statistics table, choose this option from the Type drop-down menu. The GUI displays the count and rate values for these statistics:

Column	Description
APN Name	The name of the Access Point Name (APN).
APN Index	A unique numerical identifier for the APN.

Column	Description
Sampling Interval in Minutes: 3	Throughput statistics on the APN for a duration of 3 minutes.
Sampling Interval in Minutes: 5	Throughput statistics on the APN for a duration of 5 minutes.
Upstream Packets	Rate (per second) of upstream packets sent on this APN during the last sampling period.
Upstream Bytes	Rate (per second) of upstream bytes sent on this APN during the last sampling period.
Downstream Packets	Rate (per second) of downstream packets sent on this APN during the last sampling period.
Downstream Bytes	Rate (per second) of downstream bytes sent on this APN during the last sampling period.
Data age (minutes)	The difference in minutes between the time when the data was collected and retrieved. This is the time that has elapsed after the previous collection or update of the data.

IP Local Pool Config



Note

For toolbar details, see [Using the Toolbar, page 11-5](#).

The IP Local Pool Config subtab shows IP addresses for GGSN nodes and contains:

Column	Description
Name	Name of the IP local pool.
Addresses	Low—The first IP address of the range of IP addresses contained by this pool entry.
	High—The last IP address of the range of IP addresses mapped by this pool entry.
	Free—The number of IP addresses available for use within the range of IP addresses.
	In Use—The number of IP addresses being used within the range of IP addresses.

IP Local Pool Stats

**Note**

For toolbar details, see [Using the Toolbar, page 11-5](#).

The IP Local Pool Stats subtab shows IP addresses and IP addresses in use for GGSN nodes and contains:

Column	Description
Name	Name of the IP local pool.
Addresses	Free—The number of IP addresses available for use in this IP local pool.
	In Use—The number of IP addresses being used in this IP local pool.
	Maximum in Use—The maximum number of used addresses in an IP local pool since pool creation, since the system was restarted, or since this object was reset, whichever occurred last.

Displaying PWE3 Real-Time Statistics

The MWTM enables you to display PWE3 real-time statistics in the MWTM web interface. Because the MWTM client also displays these statistics and the GUIs for the web and client interfaces are so similar, the PWE3 real-time statistics are described in [Viewing PWE3 Statistics, page 8-121](#).

Displaying TDM Real-Time Statistics

The MWTM enables you to display TDM real-time statistics in the MWTM web interface. Because the MWTM client also displays these statistics and the GUIs for the web and client interfaces are so similar, the TDM real-time statistics are described in [Viewing TDM Statistics, page 8-103](#).



CHAPTER 12

Managing Reports

At scheduled intervals, you can configure the Cisco Mobile Wireless Transport Manager (MWTM) to gather critical information from network objects that it detects. The MWTM uses that information to calculate statistics (accounting statistics, inventory statistics, and so on) and generates reports based on those statistics.

This chapter contains:

- [Generating Reports, page 12-1](#)
- [Viewing Reports, page 12-6](#)
- [Locating Stored ITP Reports, page 12-63](#)
- [Customizing ITP Report Preferences, page 12-65](#)

Generating Reports

Using CLI commands, there are two types of reports that you can generate:

- Continuous reports that use cron jobs to run at specified intervals. You generate these reports with the “mwtm statreps” commands (see [Viewing Enabled and Disabled Status for Continuous Reports on the Web, page 12-2](#)). Once you generate a continuous report, it will run at the specified intervals until you disable it with the appropriate CLI command.
- Custom reports that you create one-time on demand. You generate these reports with the “mwtm stats” commands (see [Generating Custom Statistics Reports, page 12-3](#)).

Both types of reports contain the same data.

To generate reports:

-
- Step 1** Decide:
- a. What type of report you want to generate: continuous or custom;
 - b. What specific report you want to generate data for (for example, GTT statistics, MLR statistics, application server statistics, etc.).
- Step 2** Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).
- Step 3** Enter:
- ```
cd /opt/CSCOsgm/bin
```

- Step 4** Enter the CLI command that starts the report generation. For example, to generate continuous GTT statistics, enter:

```
./mwtm statreps gtt
```

To determine which CLI command generates which report, see [Viewing Enabled and Disabled Status for Continuous Reports on the Web, page 12-2](#) or [Generating Custom Statistics Reports, page 12-3](#).

- Step 5** (Optional) View the generated report using the MWTM web interface. For example, to view a continuous GTT statistics report, open the web interface and navigate to Reports > Accounting > GTT. For details, see [Viewing Reports, page 12-6](#).

## Viewing Enabled and Disabled Status for Continuous Reports on the Web

The main Reports page on the MWTM web interface shows all continuous reports and whether or not they are being generated. To access the main Reports page:

- Step 1** Do one of the following:

- In a Web browser, launch the MWTM Web interface (see [Accessing the MWTM Web Interface, page 11-1](#)). In the navigation tree, click **Reports**.
- From the MWTM client, in the MWTM main window, choose **View > Web > Reports**.

The Reports page in the content area shows the Report Type and the Data Collection Status (enabled or disabled).

**Figure 12-1** Report Parameters and Timers

| Report Type  | Data Collection Status | Last Start | Last Finish      |
|--------------|------------------------|------------|------------------|
| AS           | Disabled               | Unknown    | Unknown          |
| ASP          | Disabled               | Unknown    | Unknown          |
| Events       | Enabled                | Unknown    | Unknown          |
| GTT          | Disabled               | Unknown    | Unknown          |
| IP Addresses | Enabled                | Unknown    | Unknown          |
| Link         | Disabled               | Unknown    | Unknown          |
| Linkset      | Disabled               | Unknown    | Unknown          |
| MLR          | Disabled               | Unknown    | Unknown          |
| MSU Rates    | Disabled               | Unknown    | Unknown          |
| MTP3         | Disabled               | Unknown    | Unknown          |
| Point Codes  | Enabled                | Unknown    | Unknown          |
| RAN          | Enabled                | N/A        | 10/17/2008 13:30 |

- Step 2** Click the plus (+) sign to expand a Report Type. If you have generated a report (using the associated CLI command) a green status ball and the word “Enabled” appear in the Data Collection Status column. If you have not generated a report, a red status ball and the word “Disabled” appears.



**Note** Clicking a Report Type takes you directly to the report data page.

To see which CLI command enables or disables a report, click the Disabled or Enabled link (if available). A popup window appears with the associated command. As the root user, you can log in to the MWTM server and run the specified command to enable the report.



**Note** For more descriptions of CLI commands, see [Appendix B, “Command Reference.”](#)

## Generating Custom Statistics Reports

In the MWTM, you can use custom CLI commands to create summary reports of custom statistics and open them as an export file. To create a custom report:

- Step 1** Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).
- Step 2** Enter:
- ```
# cd /opt/CSCOSgm/bin
```
- Step 3** Based on the type of custom report you want to generate, enter one of these commands to enable the report:



Note For complete information about these commands, see [Appendix B, “Command Reference.”](#)

Custom Report	Command
Application server and application server processes custom statistics	mwtm xuastats
GTT accounting statistics	mwtm gttstats
Link and linkset summary	mwtm linkstats
MLR statistics	mwtm mlrstats
MTP3 accounting statistics	mwtm accstats
MTP3 event summary	mwtm mtpevents
Q.752 statistics	mwtm q752stats

For example, if you entered the command:

```
# ./mwtm accstats mwtm-2600a.cisco.com test1 -sno
```

The MWTM generates these reports:

```
mwtmAccStats.custom.test1.2004-02-13:15.csv.zip
mwtmAccStats.custom.test1.2004-02-13:15.csv.zip
```

- Step 4** (Optional) To include or exclude specific nodes, signaling points or linksets in the report, see [Locating Stored ITP Reports, page 12-63](#).

Step 5 (First-time users only) If this is your first time using the **mwtm accstats**, **mwtm gttstats**, **mwtm mlrstats**, **mwtm mtpevents**, **mwtm q752stats**, or **mwtm xuastats** command to enable a report, you must enter the command one more time. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful accounting statistics and, if the data being collected appears valid, begins generating the report.

or

If this is your first time using the **mwtm linkstats** command to enable a report, you must enter the command two more times. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful link and linkset statistics.
- Third entry continues to calculate statistics, calculates long-term averages, and, if the data being collected appears to be valid, begins generating the report.

Thereafter, you need only enter these commands once to enable the report.

Step 6 (Optional) You can automate custom report generation using crontab. For example, to run custom MTP3 accounting statistics once per hour, enter:

```
00 * * * * /opt/CSCOs-gm/bin/mwtm accstats quiet
```

or, to run custom link statistics every 30 minutes, enter:

```
00,30 * * * * /opt/CSCOs-gm/bin/mwtm linkstats quiet
```

Step 7 You can view custom reports on the MWTM Web interface under **Reports > File Archive > Custom**. Click on the respective link in the View column to see the data in HTML, or click on a .zip file to see the data in .csv format.



Note You can only view Q.752 reports in .csv format.

The MWTM also stores custom reports in the */custom* directory (for details, see [Locating Stored ITP Reports, page 12-63](#).)

Including or Excluding Specified Objects in ITP Reports

You can include or exclude specific nodes, signaling points, or linksets in ITP reports by creating user-defined files. The nodes, signaling points, and/or linksets that you specify in these files will be included or excluded from enabled MWTM statistics reports and in custom reports enabled with the **default** keyword (or no *node-list* keyword at all), which include:

Command	Filename ¹
mwtm linkstats	nodes.include.linkstats or nodes.include
	nodes.exclude.linkstats or nodes.exclude
	linksets.include.linkstats or linkstats.include
	linksets.exclude.linkstats or linkstats.exclude

Command	Filename ¹
mwtm q752stats	nodes.include.q752stats or nodes.include
	nodes.exclude.q752stats or nodes.exclude
	linksets.include.q752stats or linkstats.include
	linksets.exclude.q752stats or linkstats.exclude
mwtm accstats	nodes.include.accstats or nodes.include
	nodes.exclude.accstats or nodes.exclude
	linksets.include.accstats or linkstats.include
	linksets.exclude.accstats or linkstats.exclude
	filter.include.accstats or filter.include ²
mwtm gttstats	nodes.include.gttstats or nodes.include
	nodes.exclude.gttstats or nodes.exclude
	linksets.include.gttstats or linkstats.include
	linksets.exclude.gttstats or linkstats.exclude
	filter.include.gttstats or filter.include ³
mwtm mtpevents	nodes.include.mtpevents or nodes.include
	nodes.exclude.mtpevents or nodes.exclude
mwtm mlrstats	nodes.include.mlrstats or nodes.include
	nodes.exclude.mlrstats or nodes.exclude
mwtm xuastats	nodes.include.xuastats or nodes.include
	nodes.exclude.xuastats or nodes.exclude

1. Files on the command line override system files. For example, nodes.include.accstats overrides nodes.include.
2. Format is opc:dpc (originating point code and destination point code).
3. Format is gta:sel (global title address and selector).

**Note**

The MWTM processes the include files first, then the exclude files.

When creating user-defined files, remember that if you installed the MWTM in:

- The default directory, */opt*, then the user-defined file resides in */opt/CSCOs/gm/reports/etc/<user-defined file>*.

A different directory, or if you moved the report files directory using the **mwtm repdir** command, then the */reports/etc/<user-defined file>* resides in that directory.

- Wildcard matching is not supported.
- If a node, signaling point, or linkset appears in both the *include* file and the *exclude* file, it is excluded. That is, excluding an object overrides including the same object.
- If you specify a special *include* file on the **mwtm accstats**, **mwtm gttstats**, **mwtm linkstats**, **mwtm mlrstats**, **mwtm mtpevents**, **mwtm q752stats**, or **mwtm xuastats** command, the MWTM ignores the *include* or *exclude* file.

When creating a *nodes.include* or *nodes.exclude* file:

Each line in the file must contain a single node name, or node name and signaling point name, separated by a colon (:) that matches exactly the real, fully qualified name of the node; for example:

```
mwtm-75-59a.cisco.com
mwtm-26-51a.cisco.com
```

To include a specific signaling point, specify the node name and signaling point:

```
mwtm-75-59a.cisco.com;net0
mwtm-26-51a.cisco.com;net0
```

When creating a *linksets.include* or *linksets.exclude* file:

Each line in the file must contain a single linkset name that matches exactly the real, fully qualified linkset name of the linkset, including the node name and signaling point name; for example:

```
mwtm-75-59a.cisco.com;net0:linkset2
mwtm-26-51a.cisco.com;net0:linkset1
```

When creating a *filter.include* file:

Each line in the file must contain a single originating point code and destination point code (for accounting statistics) that matches the current point code format; or a single phone number and selector name (for GTT statistics); for example:

```
1.2.3:5.6.7
8882214040:Selector_1
```

Viewing Reports

Once you generate reports using the CLI commands, you can view them using the MWTM web interface. You can view reports for all objects of a specific type (for example, all link reports for all links) or, you can view reports for a specific object (for example, all link reports for a specific link).

You can access reports in the MWTM web interface through these categories:

Category	Report Type	Related Content
Reports > Statistics	AS	Application Server Reports, page 12-9
	ASP	Application Server Process Reports, page 12-12
	Events	The event metrics reports are applicable for RAN-O and ITP networks. You can find information on event metrics reports in the “Managing Events” chapter (see Viewing the Event Metrics Report on the Web, page 9-30).
	Link	Link Reports, page 12-17
	Linkset	Linkset Reports, page 12-23
	MLR	MLR Reports, page 12-27
	MSU Rates	MSU Rates Reports, page 12-32
	RAN	RAN Reports, page 12-34

Category	Report Type	Related Content
Reports > Accounting	GTT	GTT Accounting Reports, page 12-41
	MTP3	MTP3 Accounting Reports, page 12-42
	AS/ASP	AS/ASP Accounting Reports, page 12-44
File Archive > Events	N/A	Archived event reports are applicable for RAN-O and ITP networks. You can find information on archived event reports in the “Managing Events” chapter (see Viewing Archived Event Files on the Web, page 9-30).
File Archive > Reports	Custom	Custom Archived Reports, page 12-46
	Daily	Daily Archived Reports, page 12-48
	Hourly	Hourly Archived Reports, page 12-49
	Rolling	Rolling Archived Reports, page 12-49
	AS	Application Server Archived Reports, page 12-50
	ASP	Application Server Process Archived Reports, page 12-50
	GTT	GTT Accounting Archived Reports, page 12-51
	Link	Link Archived Reports, page 12-52
	Linkset	Linkset Archived Reports, page 12-52
	MLR	Daily MLR Statistics Archived Reports, page 12-57
	MSU	MSU Archived Reports, page 12-54
	MTP3/AS	MTP3/AS Archived Reports, page 12-55
	Point Codes	Point Codes Archived Reports, page 12-58
	Q752	Q.752 Hourly Archived Reports, page 12-58

**Note**

File Archive reports contain the most data. Accounting and statistics reports contain a subset of the same data.

To view a Web report:

Step 1 For all objects of a specified type:

- From the MWTM web navigation tree, in **Reports** or **File Archive**, click the type of report you want to view in the web navigation tree; for example, if you want to view current link reports, select **Reports > Statistics > Link**. All link reports appear.

For a single object of a specified type do one of the following. From the MWTM:

- Web navigation tree, in **DEFAULT View**, click a node or drill down to click an object in a node. In the content area in the right pane, click the **Reports** tab. Reports appear for the active object only.
- Client, right-click an object and click **Latest Reports**. The Reports tab in the MWTM web interface opens for the active object only.

Figure 12-2 MWTM Web Interface—Reports

Mobile Wireless Transport Manager
ems-svr276 (IP-RAN ITP CSG1 CSG2 GGSN BWG HA)

Version 6.1.0.17
Help | Preferences

Location **DEFAULT** View → sgm-26-91g

Details Status Contributors Notes Troubleshooting Events Alarms Syslog Performance Trap Settings MTP3 Errors **Reports**

Link Hourly Report 10/29/2008 11:00 - 10/29/2008 13:00 Page 1 of 3 (274 entries)

Filtered by Node: sgm-26-91g

Type: Link Hourly Duration: Last Hour Page Size: 100

Date	Network Name	Signaling Point	Link	Type	Send Utilization (%)	Long-Term Send Utilization (%)	Receive Utilization (%)	Long Term Receive Utilization (%)	Send MSUs	Receive MSUs	Congestion %	Hourly In-Service (%)	Long Term In-Service (%)
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/9]	SCTP	0.00	0.00	0.00	0.00	133	120	0.00	100.000	99.994
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/8]	SCTP	0.00	0.00	0.00	0.00	132	119	0.00	100.000	99.995
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/7]	SCTP	0.00	0.00	0.00	0.00	133	120	0.00	100.000	99.995
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/6]	SCTP	0.00	0.00	0.00	0.00	133	120	0.00	100.000	99.995
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/5]	SCTP	0.00	0.00	0.00	0.00	134	120	0.00	100.000	99.995
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/4]	SCTP	0.00	0.00	0.00	0.00	119	119	0.00	100.000	99.994
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/3]	SCTP	0.00	0.00	0.00	0.00	120	120	0.00	100.000	99.995
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/2]	SCTP	0.00	0.00	0.00	0.00	120	120	0.00	100.000	99.995
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/1]	SCTP	0.00	0.00	0.00	0.00	120	120	0.00	100.000	99.994
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591b3/0]	SCTP	0.00	0.00	0.00	0.00	133	120	0.00	100.000	99.995
10/29/2008 12:00	ansinet3	1.8.3:ansinet3	[2691g_to_7591a3/9]	SCTP	0.00	0.00	0.00	0.00	120	120	0.00	100.000	99.955

**Note**

In the MWTM web interface, if you do not enable data collection on the active report, a red ball  and the words Data Collection Disabled appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

- Step 2** Choose the **Type** and **Duration** from the drop-down lists; for example, if you wanted to view hourly link reports for the last 12 hours, choose **Link Hourly** from the Type list and **Last 12 Hours** from the Duration list.
- Step 3** (Optional) For most Statistics and Accounting reports, to customize the date or time range (or both) click the Customize icon. 
- Step 4** Click the green arrow to run the report. If you change the Type or Duration, an information message appears:
Click the green arrow to show the selected report.
- Step 5** To disable this error message, click **Hide Message**. To display the message again, click the **Information** icon. 
- Step 6** (Optional) For Statistics and Accounting reports, to export the report as a .csv file, click the **Export** icon.  For detailed information on content within exported reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>

**Note**

For more details on using the MWTM web interface, see [Chapter 11, “Accessing Data from the Web Interface.”](#)

Once you open a report, you can drill down to:

- See raw data for an object (helpful in diagnosing problems)—Click the first **Filter** icon  located at the beginning of a row, next to the Date column.
- Drill down under an object—Click the **Filter** icon  located on the left of the object. Drilling down shows objects beneath other objects.

**Note**

To navigate to the Details tab for an object, click the underlined object in the report; for example, to go to the Details tab for a node, click the underlined node in the reports table.

**Tip**

For details on web toolbars and icons, see [Using the Toolbar, page 11-5](#).

Viewing Statistics Reports

You can view any of the following statistics reports:

- [Application Server Reports, page 12-9](#)
- [Application Server Process Reports, page 12-12](#)
- [Link Reports, page 12-17](#)
- [Linkset Reports, page 12-23](#)
- [MLR Reports, page 12-27](#)
- [MSU Rates Reports, page 12-32](#)
- [RAN Reports, page 12-34](#)

Application Server Reports

The xUA statistics encompass Message Transfer Part 3 User Adaptation (M3UA) and Signaling Connection Control Part User Adaptation (SUA). xUA connects application servers to SS7 networks.

You can view summary reports of hourly and daily application server statistics. You can also export the reports.

This section covers:

- [Hourly Application Server Reports, page 12-9](#)
- [Daily Application Server Reports, page 12-10](#)
- [Daily Application Server Peaks Reports, page 12-11](#)
- [Daily Application Server Archived Reports, page 12-50](#)
- [Hourly Application Server Archived Reports, page 12-50](#)

Hourly Application Server Reports

You can view hourly summaries of application server statistics for all application servers that the MWTM detects for the specified date and hour range. The AS Hourly Report page shows summary reports of hourly application server statistics by date and hour.

The AS Hourly Report table is sorted based on the information in the Packets From MTP3 column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).

**Note**

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the application server.
Network Name	Name of the network for the application server.
Signaling Point	Name of the signaling point for the application server.
AS	Name of the application server.
Packets From MTP3	Total number of packets that the application server received, sent from the MTP3 layer.
Packets To ASPs	Total number of packets that the application server sent to the application server processes.

Daily Application Server Reports

You can view a daily summary of statistics for all application servers that the MWTM detects for a specified date range. The AS Daily Report page shows summary reports of daily application server statistics that are archived by date and hour.

The AS Daily Report table is sorted based on the information in the Packets From MTP3 column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).

**Note**

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the application server.
Network Name	Name of the network for the application server.
Signaling Point	Name of the signaling point for the application server.

Field or Column	Description
AS	Name of the application server.
Packets From MTP3	Total number of packets that the application server receives from the MTP3 layer for the specified date.
Peak From MTP3	Highest hourly Packets From MTP3 for the application server for the specified date.
Peak From Hour	Hour in which the Peak From MTP3 for the application server occurred for the specified date. Click the hour to see the AS Hourly Report for the chosen application server and hour.
Packets To ASPs	Total number of packets that the application server sent to the application server processes for the specified date.
Peak To ASPs	Highest hourly Packets To ASPs for the application server for the specified date.
Peak To Hour	Hour in which the Peak To ASPs for the application server occurred for the specified date. Click the hour to see the AS Hourly Report for the chosen application server and hour.

Daily Application Server Peaks Reports

You can view an application server statistics Peaks Report to see peak values for each day and the hour in which each peak value occurred. The AS Peaks Daily Report page shows summary reports of daily application server peak statistics by date and hour.

The AS Peaks Daily Report table is sorted based on the information in the Peak From MTP3 column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appears next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the application server.
Network Name	Name of the network for the application server.
Signaling Point	Name of the signaling point for the application server.
AS	Name of the application server that recorded the peak value.
Peak From MTP3	Highest hourly Packets From MTP3 for the application server for the last 30 days.

Field or Column	Description
Peak From Hour	Hour in which the Peak From MTP3 for the application server occurred. Click the hour to see the AS Hourly Report for the chosen application server and hour.
Peak To ASPs	Highest hourly Packets To ASPs for the application server for the last 30 days.
Peak To Hour	Hour in which the Peak To ASPs for the application server occurred. Click the hour to see the AS Hourly Report for the chosen application server and hour.

Application Server Process Reports

You can view summary reports of hourly and daily xUA statistics. You can also export the reports.

The xUA statistics encompass Message Transfer Part 3 User Adaptation (M3UA) and Signalling Connection Control Part User Adaptation (SUA). xUA connects application servers to SS7 networks.

This section covers:

- [Hourly Application Server Process Reports, page 12-12](#)
- [Daily Application Server Process Reports, page 12-13](#)
- [Daily Application Server Process Peaks Reports, page 12-15](#)
- [Daily Application Server Process MTP3 Peaks Reports, page 12-16](#)

Hourly Application Server Process Reports

You can view hourly summaries of statistics for all application server processes that the MWTM detects on the specified date and hour. The ASP Hourly Report page shows summary reports of hourly application server process statistics by date and hour.

The ASP Hourly Report table is sorted based on the information in the Packets From ASP column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the application server process.
ASP	Name of the application server process.
Packets From ASP	Total number of packets that the application server process send for the specified date and hour.

Field or Column	Description
Packets To ASP	Total number of packets sent to the application server process for the specified date and hour.
Packets From MTP3	Total number of packets that the application server process received from the MTP3 layer for the specified date and hour.
Packets To MTP3	Total number of packets the application server process sent to the MTP3 layer for the specified date and hour.
Send Errors	Total number of errors that occurred when sending packets to the application server process for the specified date and hour.
Receive Errors	Total number of errors that occurred when receiving packets from the application server process for the specified date and hour.

Daily Application Server Process Reports

You can view a daily summary of statistics for all application server processes that the MWTM detects on a specified date. The ASP Daily Report page shows summary reports of daily application server process statistics, archived by date and hour.

The ASP Daily Report table is sorted based on the information in the Packets From ASP column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns](#), page 5-24).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the application server process.
ASP	Name of the application server process.
Packets From ASP	Total number of packets that the application server process sent for the specified date.
Peak From ASP	Highest hourly Pkts From ASP for the application server for the specified date.
Peak From Hour	Hour in which the Peak From ASP for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Packets To ASP	Total number of packets that the application server sent to the application server processes for the specified date.
Peak To ASP	Highest hourly Pkts To ASP for the application server for the specified date.

Field or Column	Description
Peak To Hour	Hour in which the Peak To ASP for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Send Errors	Total number of errors that occurred when sending packets to the application server processes for the specified date.
Peak Send Errors	Highest hourly Send Errors for the application server for the specified date.
Peak Send Hour	Hour in which the Peak Send Errors for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Receive Errors	Total number of errors that occurred when receiving packets from the application server processes for the specified date.
Peak Receive Errors	Highest hourly receive errors for the application server for the specified date.
Peak Receive Hour	Hour in which the peak receive errors for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.

Daily Application Server Process MTP3 Reports

The ASP MTP3 Daily Report page shows a daily summary of MTP3 statistics for all application server processes that the MWTM detects on a specified date. The ASP MTP3 Daily Report page shows a summary report of daily application server process MTP3 statistics by date and hour.

The ASP MTP3 Daily Report table is sorted based on the information in the Packets From MTP3 column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appears next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the application server process.
ASP	Name of the application server process.
Packets From MTP3	Total number of packets that the application server process receives from the MTP3 layer for the specified date.

Field or Column	Description
Peak From MTP3	Highest hourly Packets From MTP3 for the application server process for the specified date.
Peak From Hour	Hour in which the Peak From MTP3 for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Packets To MTP3	Total number of packets sent to the MTP3 layer by the application server process for the specified date.
Peak To MTP3	Highest hourly Packets To MTP3 for the application server process for the specified date.
Peak To Hour	Hour in which the Peak To MTP3 for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Send Errors	Total number of errors that occurred when sending packets to the MTP3 layer for the specified date.
Peak Send Errors	Highest hourly Send Errors for the application server process for the specified date.
Peak Send Hour	Hour in which the Peak Send Errors for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Receive Errors	Total number of errors that occurred when receiving packets from the MTP3 layer for the specified date.
Peak Receive Errors	Highest hourly Receive Errors for the application server process for the specified date.
Peak Receive Hour	Hour in which the Peak Receive Errors for the application server process occurred for the specified date. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.

Daily Application Server Process Peaks Reports

You can view a report of the statistics peaks for the application server process. The peaks report shows peak values for each day of the last 30 days, and the hour in which each peak occurred. The ASP Peaks Daily Report page shows a summary report of the daily application server process peak statistics by date and hour.

The ASP Peaks Daily Report table is sorted based on the information in the Peak From ASP column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns](#), page 5-24).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the application server process.
ASP	Name of the application server process that recorded the peak value.
Peak From ASP	Highest hourly Packets From ASP for the application server for the chosen day.
Peak From Hour	Hour in which the Peak From ASP for the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Peak To ASP	Highest hourly Packets To ASP for the application server for the chosen day.
Peak To Hour	Hour in which the Peak To ASP for the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Peak Send Errors	Highest hourly Send Errors for the application server for the last 30 days.
Peak Send Hour	Hour in which the Peak Send Errors for the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Peak Receive Errors	Highest hourly Receive Errors for the application server for the last 30 days.
Peak Receive Hour	Hour in which the Peak Receive Errors for the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.

Daily Application Server Process MTP3 Peaks Reports

You can view a peaks report of the application server process MTP3 statistics. The peaks report shows peak values for each day and the hour in which each peak value occurred. The ASP MTP3 Peaks Daily Report page shows summary reports of the daily application server process MTP3 peak statistics by date and hour.

The ASP MTP3 Peaks Daily Report table is sorted based on the information in the Peak From MTP3 column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).

**Note**

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date on which the peak values occurred.
Node	Name of the node for the application server process.
ASP	Name of the application server process that recorded the peak value.
Peak From MTP3	Highest hourly Packets From MTP3 to the application server process for the chosen day.
Peak From Hour	Hour in which the Peak From MTP3 to the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Peak To MTP3	Highest hourly Packets to MTP3 from the application server process for the chosen day.
Peak To Hour	Hour in which the Peak to MTP3 from the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Peak Send Errors	Highest hourly Send Errors for the application server process for the chosen day.
Peak Send Hour	Hour in which the Peak Send Errors for the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.
Peak Receive Errors	Highest hourly Receive Errors for the application server process for the chosen day.
Peak Receive Hour	Hour in which the Peak Receive Errors for the application server process occurred for the chosen day. Click the hour to see the ASP Hourly Report for the chosen application server process and hour.

Link Reports

You can view summary reports of hourly and daily statistics for links, and export the reports.

This section covers:

- [Hourly Link Reports, page 12-18](#)
- [Daily Link Reports, page 12-19](#)

- [Daily Link Peaks Reports, page 12-21](#)
- [Link Multi-Day Utilization Report, page 12-22](#)

Hourly Link Reports

You can view hourly summaries of statistics for all links or a specific link that the MWTM detected on the specified date and hour. The Link Hourly Report page shows summary reports of hourly link statistics by date and hour.

The Link Hourly Report table is sorted based on the information in the Send Utilization or Send Erlangs column; however, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the link.
Network Name	Name of the network for the link.
Signaling Point	Name of the signaling point for the link.
Link	Name of the link.
Type	Type of link. Possible link types are: • HSL—Uses the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol. • SCTP—Uses the Stream Control Transmission Protocol (SCTP) IP transport protocol. • Serial—Uses the serial SS7 signaling protocol. • Virtual—A virtual link that connects signaling point instances that run on the same node. The MWTM does not poll virtual links; nor does it display real-time data or accounting statistics for virtual links.
Send Utilization or Send Erlangs	Average Send Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date and hour. If you do not set the planned send capacity for the SCTP link, then <code>NoCap</code> appears in the field.
Receive Utilization or Receive Erlangs	Average Receive Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date and hour. If you do not set the planned receive capacity for the SCTP link, then <code>NoCap</code> appears in the field.

Field or Column	Description
Long Term Send Utilization or Long Term Send Erlangs	Long-term average Send Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the link, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned send capacity for the SCTP link, then NoCap appears in the field.
Long Term Receive Utilization or Long Term Receive Erlangs	Long-term average Receive Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the link, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned receive capacity for the SCTP link, then NoCap appears in the field.
Send MSUs	Total number of MTP3 message signal units (MSUs) sent on the specified date and hour.
Receive MSUs	Total number of MTP3 MSUs received on the specified date and hour.
Congestion %	Percentage of time the link was congested on the specified date and hour.
Hourly In-Service	Percentage of time the link was in service on the specified date and hour.
Long Term In-Service	Average percentage of time the link was in service since MWTM polling began for the link, or since the MWTM last reset the averages as a result of bad data.

Daily Link Reports

You can view daily summaries of statistics for all links or for a specific link that the MWTM detected on the specified date and hour. The Link Daily Report page shows summary reports of daily link statistics by date and hour.

The Link Daily Report table is sorted based on the information in the Avg Send Utilization or Avg Send Erlangs column. However, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words **Data Collection Disabled** appears next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then **MathError** appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the link.
Network Name	Name of the network for the link.
Signaling Point	Name of the signaling point for the link.
Link	Name of the link.

Field or Column	Description
Type	Type of link. Possible link types are: • HSL—The link uses the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol. • SCTP—The link uses the Stream Control Transmission Protocol (SCTP) IP transport protocol. • Serial—The link uses the serial SS7 signaling protocol. • Virtual—The link is a virtual link, which connects signaling point instances running on the same node. The MWTM does not poll virtual links, nor does it display real-time data or accounting statistics for virtual links.
Avg Send Utilization or Avg Send Erlangs	Average Send Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date. If you do not set the planned send capacity for the SCTP link, then NoCap appears in the field.
Peak Send Utilization or Peak Send Erlangs	Highest hourly Average Send Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date.
Peak Send Hour	Hour in which the Peak Send Utilization for the link occurred for the specified date. Click the hour to see the Link Hourly Report for the chosen link and hour.
Long Term Send Utilization or Long Term Send Erlangs	Long-term average Send Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the link, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned send capacity for the SCTP link, then NoCap appears in the field.
Avg Receive Utilization or Avg Receive Erlangs	Average Receive Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date. If you do not set the planned receive capacity for the SCTP link, then NoCap appears in the field.
Peak Receive Utilization or Peak Receive Erlangs	Highest hourly Average Receive Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date.
Peak Receive Hour	Hour in which the Peak Receive Utilization for the link occurred for the specified date. Click the hour to see the Link Hourly Report for the chosen link and hour.
Long Term Receive Utilization or Long Term Receive Erlangs	Long-term average Receive Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the link, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned receive capacity for the SCTP link, then NoCap appears in the field.

Field or Column	Description
Send MSUs	Total number of MTP3 MSUs sent on the specified date.
Receive MSUs	Total number of MTP3 MSUs received on the specified date.
Avg Congestion %	Average percentage of time the link was congested on the specified date.
Daily In-Service	Average percentage of time the link was in service on the specified date.
Long Term In-Service	Average percentage of time the link was in service since MWTM polling began for the link, or since the MWTM last reset the averages as a result of bad data.
Daily Low In-Service	Lowest hourly in-service percentage for the link for the specified date.
Low Srv Hour	Hour in which the lowest in-service percentage occurred for the specified date.

Daily Link Peaks Reports

You can view a daily link statistics peaks report using the Link Peaks Daily Report page. The peaks report shows peak values for each day and the hour in which each peak value occurred.

The Link Peaks Daily table is sorted based on the information in the Peak Send Utilization or Peak Send Erlangs column. However, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the link.
Network Name	Name of the network for the link.
Signaling Point	Name of the signaling point for the link.
Link	Name of the link that recorded the peak value.
Type	Type of link. Possible link types are: • HSL—The link uses the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol. • SCTP—The link uses the Stream Control Transmission Protocol (SCTP) IP transport protocol. • Serial—The link uses the serial SS7 signaling protocol. • Virtual—The link is a virtual link, which connects signaling point instances running on the same node. The MWTM does not poll virtual links, nor does it display real-time data or accounting statistics for virtual links.

Field or Column	Description
Peak Send Utilization or Peak Send Erlangs	Peak Send Utilization for the link for the chosen day, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command).
Peak Send Hour	Hour in which the Peak Send Utilization occurred for the chosen day. Click the hour to see the Link Hourly Report for the chosen link and hour.
Peak Receive Utilization or Peak Receive Erlangs	Peak Receive Utilization for the link for the chosen day, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command).
Peak Receive Hour	Hour in which the Peak Receive Utilization occurred for the chosen day. Click the hour to see the Link Hourly Report for the chosen link and hour.
Send MSUs	Total number of MTP3 MSUs sent on the specified date.
Receive MSUs	Total number of MTP3 MSUs received on the specified date.

Link Multi-Day Utilization Report

The Link Multi-Day Report page shows send and receive utilization percentages for all links for the last three or five days.

The Link Multi-Day table is sorted based on the information in the Avg Send Utilization column. However, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns](#), page 5-24).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Node	Name of the node for the link.
Network Name	Name of the network for the link.
Signaling Point	Name of the signaling point for the link.
Link	Name of the link.

Field or Column	Description
Avg. Send Utilization	Send Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for each of the last five days. If you do not set the planned send capacity for the SCTP link, then <code>NoCap</code> appears in the field.
Avg. Receive Utilization	Receive Utilization for the link, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for each of the last five days. If you do not set the planned receive capacity for the SCTP link, then <code>NoCap</code> appears in the field.

Linkset Reports

You can view summary reports of hourly and daily statistics for linksets, and export the reports.

This section covers:

- [Hourly Linkset Reports, page 12-23](#)
- [Daily Linkset Reports, page 12-24](#)
- [Daily Linkset Peaks Reports, page 12-26](#)

Hourly Linkset Reports

You can view hourly summaries of statistics for all linksets or for a specific linkset that the MWTM detected on the specified date and hour. The Linkset Hourly Report page shows summary reports for all archived MWTM hourly linkset statistics by date and hour.

The Linkset Hourly Report table is sorted based on the information in the Hourly In-Service column, then by the information in the Send Utilization or Send Erlangs column. However, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Column	Description
Date	Date and time of the report.
Node	Name of the node for the linkset.
Network Name	Name of the network for the linkset.
Signaling Point	Name of the signaling point for the linkset.
Linkset	Name of the linkset.

Column	Description
Hourly In-Service	Percentage of time the linkset was in service on the specified date and hour.
Long Term In-Service	Average percentage of time the linkset was in service since the MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data.
Send Utilization or Send Erlangs	Average Send Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date and hour. If you do not set the planned send capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.
Long Term Send Utilization or Long Term Send Erlangs	Long-term average Send Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned send capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.
Receive Utilization or Receive Erlangs	Average Receive Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date and hour. If you do not set the planned receive capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.
Long Term Receive Utilization or Long Term Receive Erlangs	Long-term average Receive Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned receive capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.

Daily Linkset Reports

You can view daily summaries of statistics for all linksets or for a specific linkset that the MWTM detected on the specified date and hour. The Linkset Daily Report page shows summary reports of all archived MWTM daily linkset statistics by date and hour.

The Linkset Daily Report table is sorted based on the information in the Daily In-Service column, then by the information in the Avg Send Utilization or Avg Send Erlangs column. You can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words **Data Collection Disabled** appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then **MathError** appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the linkset.
Network Name	Name of the network for the linkset.
Signaling Point	Name of the signaling point for the linkset.
Linkset	Name of the linkset.
Daily In-Service	Average percentage of time the linkset was in service on the specified date.
Long Term In-Service	Average percentage of time the linkset was in service since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data.
Daily Low In-Service	Lowest hourly in-service percentage for the linkset for the specified date.
Low Srv Hour	Hour in which the lowest in-service percentage occurred for the specified date.
Avg Send Utilization or Avg Send Erlangs	Average Send Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date. If you do not set the planned send capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.
Peak Send Utilization or Peak Send Erlangs	Highest hourly Average Send Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date.
Peak Send Hour	Hour in which the Peak Send Utilization for the linkset occurred for the specified date. Click the hour to see the Link Hourly Report for all links associated with the chosen linkset for the chosen hour.
Long Term Send Utilization or Long Term Send Erlangs	Long-term average Send Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned send capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.
Avg Receive Utilization or Avg Receive Erlangs	Average Receive Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date. If you do not set the planned receive capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.
Peak Receive Utilization or Peak Receive Erlangs	Highest hourly Average Receive Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command) for the specified date.

Field or Column	Description
Peak Receive Hour	Hour in which the Peak Receive Utilization for the linkset occurred for the specified date. Click the hour to see the Link Hourly Report for all links associated with the chosen linkset for the chosen hour.
Long Term Receive Utilization or Long Term Receive Erlangs	Long-term average Receive Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data. If you do not set the planned receive capacity for one or more of the SCTP links associated with the linkset, then NoCap appears in the field.

Daily Linkset Peaks Reports

You can view a daily linkset statistics peaks report using the Linkset Peaks Daily Report page. The peaks report shows peak values for each day and the hour in which each peak value occurred.

The Linkset Peaks Daily Report table is sorted based on the information in the Peak Send Utilization or Peak Send Erlangs column. However, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns](#), page 5-24).



Note

If you do not enable data collection on the active report, a red ball  and the words **Data Collection Disabled** appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then **MathError** appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the linkset.
Network Name	Name of the network for the linkset.
Signaling Point	Name of the signaling point for the linkset.
Linkset	Name of the linkset that recorded the peak value.
Peak Send Utilization or Peak Send Erlangs	Peak Send Utilization for the linkset for the chosen day, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command).
Peak Send Hour	Hour in which the Peak Send Utilization occurred for the chosen day. To see the Link Statistics - Hourly Report for all links associated with the chosen linkset for the chosen hour, click the hour.
Long Term Send Utilization or Long Term Send Erlangs	Long-term average Send Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data.

Field or Column	Description
Peak Receive Utilization or Peak Receive Erlangs	Peak Receive Utilization for the linkset for the chosen day, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command).
Peak Receive Hour	Hour in which the Peak Receive Utilization occurred for the chosen day. Click the hour to see the Link Hourly Report for all links associated with the chosen linkset for the chosen hour.
Long Term Receive Utilization or Long Term Receive Erlangs	Long-term average Receive Utilization for the linkset, expressed as a utilization percentage or number of Erlangs (E) (as set with the mwtm webutil command), since MWTM polling began for the linkset, or since the MWTM last reset the averages as a result of bad data.

MLR Reports

Multi-Layer SMS Routing, or MLR, is a routing scheme that enables intelligent routing of Short Message Service (SMS) mobile originated (MO) messages based on the application or service from which they originated or to which they are destined. The MLR feature can make SMS message routing decisions based on information found in the TCAP, MAP, and MAP-user layers; MAP operation codes MAP-MT-FORWARD-SM and SEND-ROUTING-INFO-FOR-SM; and ANSI TCAP and IS-41 MAP operations.

You can view a summary report of daily statistics for MLR. You can also export the reports.

Daily MLR Reports

You can view a summary report of MLR processed, aborts, continues, result invokes, rule matches, subtriggers, and triggers statistics for the MWTM on a specified date. The MLR *type* Daily Report page shows reports of all archived MWTM daily MLR processed, aborts, continues, result invokes, rule matches, subtriggers, and triggers by date.

These archived daily MLR reports are available:

- [Daily MLR Aborts Reports, page 12-27](#)
- [Daily MLR Continues Reports, page 12-28](#)
- [Daily MLR Processed Reports, page 12-29](#)
- [Daily MLR Result Invokes Reports, page 12-30](#)
- [Daily MLR RuleMatches Reports, page 12-31](#)
- [Daily MLR SubTriggers Reports, page 12-31](#)
- [Daily MLR Triggers Reports, page 12-32](#)

Daily MLR Aborts Reports

The MLR Aborts Daily Report table is sorted based on the information in the Total Aborted column. However, you can sort the table based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).

**Note**

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the signaling point.
Network Name	Name of the network for the signaling point.
Signaling Point	Name of the signaling point.
Total Aborted	Total number of MSUs aborted by MLR on the specified date.
No Resources	Number of MSUs aborted by MLR because of a shortage of resources on the specified date.
Results Blocked	Number of MSUs aborted by MLR with a result of block on the specified date.
GTI Mismatches	Number of MSUs aborted by MLR because of mis-matched GTIs on the specified date.
Addr Conv Fails	Number of MSUs aborted by MLR because of a failed GTA address conversion on the specified date.
Dest Unavails	Number of MSUs aborted by MLR because the destination was unavailable on the specified date.
No Server Aborted	Number of MSUs aborted by MLR because no server was available on the specified date.

Daily MLR Continues Reports

The MLR Continues Daily Report table is sorted based on the information in the Total Continued column. However, you can sort the table based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).

**Note**

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the signaling point.

Field or Column	Description
Network Name	Name of the network for the signaling point.
Signaling Point	Name of the signaling point.
Total Continued	Total number of MSUs returned to SCCP by MLR with a result of continue on the specified date.
Unsupp Msg Type	Number of MSUs returned to SCCP by MLR because of unsupported message types on the specified date.
Unsupp Seg SCCP	Number of MSUs returned to SCCP by MLR because of unsupported SCCP segments on the specified date.
Unsupported Msgs	Number of MSUs returned to SCCP by MLR because of parse failures resulting from unsupported messages on the specified date.
Parse Errors	Number of MSUs returned to SCCP by MLR because of parse errors on the specified date.
No Results	Number of MSUs returned to SCCP by MLR with no results on the specified date.
Result Continueds	Number of MSUs returned to SCCP by MLR with a result of continue on the specified date.
No Server Continueds	Number of MSUs returned to SCCP by MLR because no server was available on the specified date.
Result GTTs	Number of MSUs returned to SCCP by MLR with a result of GTT on the specified date.
Failed Trigs	Number of MSUs returned to SCCP by MLR because of no trigger match on the specified date.

Daily MLR Processed Reports

The MLR Processed Daily Report table is sorted based on the information in the Routed column. However, you can sort the table based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the signaling point.
Network Name	Name of the network for the signaling point.
Signaling Point	Name of the signaling point.
Routed	Total number of packets routed by MLR on the specified date.

Field or Column	Description
Total Continued	Total number of MSUs passed back to SCCP processing by MLR on the specified date.
Total Aborted	Total number of MSUs not processed by MLR because of invalid data or a blocked MSU.
MAP SMS-MOs	Number of MSUs of type GSM-MAP SMS-MO processed by MLR on the specified date.
MAP SMS-MTs	Number of MSUs of type GSM-MAP SMS-MT processed by MLR on the specified date.
MAP SRI-SMs	Number of MSUs of type GSM-MAP SRI-SM processed by MLR on the specified date.
MAP AlertScs	Number of MSUs of type GSM-MAP AlertSc processed by MLR on the specified date.
ANSI-41 SMD-PPs	Number of MSUs of type ANSI-41 SMD-PP processed by MLR on the specified date.
ANSI-41 SMS-Reqs	Number of MSUs of type ANSI-41 SMSRequest processed by MLR on the specified date.
ANSI-41 SMS-Notifys	Number of MSUs of type ANSI-41 SMSNotify processed by MLR on the specified date.
Links	Contains links to related MLR reports (Aborts, Continues, Triggers, SubTriggers, RuleMatches, and ResultInvokes). The target report is filtered by the signaling point.

Daily MLR Result Invokes Reports

The MLR Result Invokes Daily Report table is sorted based on the information in the Invokes column. However, you can sort the table based on the information in one of the columns (see [Navigating Table Columns](#), page 5-24).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the signaling point.
Network Name	Name of the network for the signaling point.
Signaling Point	Name of the signaling point.
ResultSet	Name of the result set of which this result is a member.
Result Number	Number of this result in the result set.
Invokes	Total number of times this result was invoked.

Daily MLR RuleMatches Reports

The MLR RuleMatches Daily Report table is sorted based on the information in the Matches column. However, you can sort the table based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the signaling point.
Network Name	Name of the network for the signaling point.
Signaling Point	Name of the signaling point.
RuleSet	Name of the rule set of which this rule is a member.
Rule Number	Number of this rule in the rule set.
Matches	Total number of times this rule was matched.

Daily MLR SubTriggers Reports

The MLR SubTriggers Daily Report table is sorted based on the information in the Matches column. However, you can sort the table based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the signaling point.
Network Name	Name of the network for the signaling point.
Signaling Point	Name of the signaling point.
Trigger Index	Index number associated with the trigger.
Sub Trigger Index	Index number associated with the subtrigger.

Field or Column	Description
Action	Action taken by the subtrigger. Clicking on the ruleset name highlights the the signaling point in the navigation tree and opens the MLR Trigger Config tab for the chosen ruleset.
Parameters	Parameters that control the behavior of the subtrigger.
Matches	Number of subtrigger matches with result Action Performed .

Daily MLR Triggers Reports

The MLR Triggers Daily Report table is sorted based on the information in the Matches column. However, you can sort the table based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the signaling point.
Network Name	Name of the network for the signaling point.
Signaling Point	Name of the signaling point.
Trigger Index	Index number associated with the trigger.
Action	Action taken by the trigger. Clicking on the ruleset name highlights the signaling point in the navigation tree and opens the MLR Trigger Config tab for the chosen ruleset.
Parameters	Parameters that control the behavior of the trigger.
Preliminary Matches	Preliminary count of trigger matches.
Matches	Number of trigger matches with result Action Performed .
Links	Contains links to related MLR SubTrigger reports. The target report is filtered by the signaling point.

MSU Rates Reports

You can view 15 minute, hourly and daily MSU rates reports. You can also export the reports in CSV format.

This section covers:

- [MSU Load Reports, page 12-33](#)
- [MSU Peaks Reports, page 12-33](#)

MSU Load Reports

You can view a 15 minute, hourly, or daily report of MSU load rates for all nodes that the MWTM detected in that time. The MSU Load Report provides the distribution of send and receive MSU packets, pertaining to overload thresholds for every CPU.

The MSU Load Report tables are sorted based on the information in the Date column. However, you can sort the tables based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).

Field or Column	Description
Date	Date of the report.
Node	Name of the node.
Processor Slot/Bay	The number of the slot and bay containing the processor. This number is set to zero when the platform does not support processors in multiple slots or bays.
Overloaded Threshold	Over this rate of traffic, MSU traffic handling may be impacted.
Duration % Send	Duration of time the send MSU rate is in the specified percentage.
Duration % Receive	Duration in time the receive MSU rate is in the specified percentage.

MSU Peaks Reports

You can view a 15 minute, hourly, or daily report of MSU peak rates for all nodes that the MWTM detected in that time. The MSU Peaks Report page provides information that helps you analyze the maximum send and receive rates for each processor in MSU units per second.

The MSU Peaks Report tables are sorted based on the information in the Send column. However, you can sort the tables based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).

Field or Column	Description
Date	Date of the report.
Node	Name of the node.
Processor Slot/Bay	Number of the slot and bay containing the processor. This number is set to zero when the platform does not support processors in multiple slots or bays.
Max Rate Send	This value records the highest rate of MSUs per second sent by the processor since the measurement was cleared.
Max Rate Receive	This value records the highest rate of MSU per second received by the processor since the measurement was cleared.
Threshold Acceptable	Specifies a level of traffic below which traffic is considered to be acceptable. Once the traffic rate exceeds the Warning threshold, it is not Acceptable until traffic falls below this threshold.
Threshold Warning	Specifies a level of traffic that should be avoided, but is below a level that impacts MSU routing. Once the traffic rate exceeds the Overloaded threshold, it is not considered non-impacting until the traffic falls below this threshold.

Field or Column	Description
Threshold Overloaded	Specifies a level of traffic indicating a rate that may impact MSU routing.
Duration in Acceptable Threshold Send	Rate of traffic (in seconds) sent by this processor considered as acceptable.
Duration in Acceptable Threshold Receive	Rate of traffic (in seconds) received by this processor considered as acceptable.
Duration in Warning Threshold Send	Rate of traffic (in seconds) sent by this processor considered above the acceptable level and below a level that impacts MSU routing.
Duration in Warning Threshold Receive	Rate of traffic (in seconds) received by this processor considered above the acceptable level and below a level that impacts MSU routing.
Duration in Overloaded Threshold Send	Rate of traffic (in seconds) sent by this processor at a level that may impact MSU routing.
Duration in Overloaded Threshold Receive	Rate of traffic (in seconds) received by this processor at a level that may impact MSU routing.

RAN Reports

The MWTM web interface provides network-wide RAN reports that show summaries of RAN-O utilization over a specified time period. The information is available in graphical, tabular, and CSV formats. Administrators use these reports for analysis of network-wide performance and errors for RAN backhauls and shorthauls.

For example, you can generate a report to show which backhaul links were the most heavily utilized in the last 24 hours. Then you can drill down to a specific node for closer analysis, if necessary.

To generate a network-wide RAN report:

- Step 1** In the left pane (navigation tree) of the MWTM web interface, choose **Reports > Statistics > RAN**.
- Step 2** In the tool bar of the right pane, choose a report type from the Type drop-down menu (see [Table 12-1](#) for a list of report types and their contents).
- Step 3** Choose a time range from the Duration drop-down menu or customize your own time range by clicking the Customize icon .
- Step 4** Choose an output format (Graph, Table, or CSV) from the Output drop-down menu (see [Table 12-1](#) for contents of each output type).
- Step 5** To generate the report, click the Run icon (green arrow .
- Step 6** To understand the report, click the report type listed in [Table 12-1](#) for a detailed description of the report fields.

Table 12-1 Report Contents

Report Type	Output	Contents
Backhaul Performance Daily	Graph	Minimum, maximum, and average performance data for all the RAN backhauls in the network: - Send Summary—Table summary of backhaul send data. - Receive Summary—Table summary of backhaul receive data. - Send Backhaul Performance Daily—Graph of backhaul send data. - Receive Backhaul Performance Daily—Graph of backhaul receive data.
	Table or CSV	Send and receive data, protocol type, node, backhaul, and shorthaul in tabular format.
Backhaul Errors Daily	Graph	For all the RAN backhauls in the network: - Table—Average error rate, total errors, and total GSM-Abis and UMTS-Iub errors in tabular format. - Backhaul Errors Daily—Graph that shows total errors, GSM errors, and UMTS errors.
	Table or CSV	Tabular information that shows total errors, total GSM-Abis errors, total UMTS-Iub errors, node, and backhaul.
Shorthaul Performance Daily	Graph	Minimum, maximum, and average performance data for all the RAN shorthauls in the network: Send Summary—Table summary of shorthaul send data. Receive Summary —Table summary of shorthaul receive data. Send Shorthaul Performance Daily—Graph of shorthaul send data. Receive Shorthaul Performance Daily—Graph of shorthaul receive data.
	Table or CSV	Tabular information that shows send and receive data, protocol type, node, backhaul, and shorthaul.
GSM Errors Daily	Graph	Table—Tabular data that shows total GSM error counts and average error rate over the chosen time period. GSM Errors Daily—Graph of GSM errors over the chosen time period.
	Table or CSV	Tabular information that shows total errors, total missed packets, total protocol errors, total miscellaneous errors, node, backhaul, and shorthaul.
UMTS Errors Daily	Graph	Table—Tabular data that shows total UMTS error counts and average error rate over the chosen time period. UMTS Errors Daily—Graph of UMTS errors over the chosen time period.
	Table or CSV	Tabular information that shows total errors, total protocol errors, total miscellaneous errors, node, backhaul, and shorthaul.

Backhaul Performance Daily

Output	GUI Element	Description
Graph	Node	Table column that lists nodes that contain RAN backhauls. To access details for a specific node, click a node in this column.
	Backhaul	Table column that lists the visible backhauls. To access details for a specific backhaul, click a backhaul in this column. Note The column shows a maximum of 12 backhauls by default. To change the number of visible backhauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Average Utilization	Table column that shows the average utilization of the backhaul. A value greater than 100% indicates that the backhaul is oversubscribed.
	Average	Table column that shows average bits per second for the backhaul.
	Minimum Utilization	Table column that shows the minimum utilization of the backhaul. A value greater than 100% indicates that the backhaul is oversubscribed.
	Minimum	Table column that shows minimum number of bits per second for the backhaul.
	Minimum Timestamp	Table column that shows time when the minimum bits-per-second value occurred.
	Maximum Utilization	Table column that shows the maximum utilization of the backhaul. A value greater than 100% indicates that the backhaul is oversubscribed.
	Maximum	Table column that shows maximum number of bits per second for the backhaul.
	Maximum Timestamp	Table column that shows time when the maximum bits-per-second value occurred.
	Expand to Full Screen	Click this link to open the graph in a full-screen window for better viewing.
	Minimum Bits/Sec	Y-axis labels for graphs that show minimum, average, and maximum bits per second for the visible backhauls.
	Average Bits/Sec	Note The graph shows a maximum of 12 backhauls by default. To change the number of visible backhauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Maximum Bits/Sec	
	<i>Legend</i>	Appearing below each graph, a legend of color-coded labels for each backhaul that appears in the graph.
Table, CSV	Node	Table column that lists all network nodes that contain backhauls. If Output is Table, to access performance details for a specific node, click a node in this column.
	Backhaul	Table column that lists all the backhauls in the network. If Output is Table, to access performance details for a specific backhaul, click a backhaul in this column.
	Errors	Table column that shows total error counts for each backhaul.
	Send	Table columns that show minimum, average, and maximum values and their timestamps for send traffic on the backhaul.
	Receive	Table columns that show minimum, average, and maximum values and their timestamps for receive traffic on the backhaul.

Backhaul Errors Daily

Output	GUI Element	Description
Graph	Node	Table column that lists nodes that contain RAN backhauls. To access details for a specific node, click a node in this column.
	Backhaul	Table column that lists the visible backhauls. To access details for a specific backhaul, click a backhaul in this column. Note The graph shows a maximum of 12 backhauls by default. To change the number of visible backhauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Avg. Error Rate (Per Sec)	Table column that lists the average error rate each second for the visible backhauls.
	Total Errors	Table column that lists the total number of errors (GSM and UMTS) for each visible backhaul.
	Total Errors GSM-Abis	Table column that lists the total number of GSM-Abis errors for each visible backhaul.
	Total Errors UMTS-Iub	Table column that lists the total number of UMTS-Iub errors for each visible backhaul.
	Expand to Full Screen	Click this link to open the graph in a full-screen window for better viewing.
	UMTS Errors	Y-axis labels for graphs that show total UMTS errors, total GSM errors, and a combined total of UMTS and GSM errors for the visible backhauls.
	GSM Errors	Note The graph shows a maximum of 12 backhauls by default. To change the number of visible backhauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Total Errors	
	Legend	Positioned below the graph, a legend of color-coded labels for each backhaul that appears in the graph.
Table, CSV	Lists the same information as the graph output type, but in tabular format; also includes one unique field:	
	Timestamp—identifies the time that each error value occurred for each visible backhaul.	

Shorthaul Performance Daily

Output	GUI Element	Description
Graph	Node	Table column that lists nodes that contain RAN shorthauls. To access details for a specific node, click a node in this column.
	Backhaul	Table column that lists the visible backhauls. To access details for a specific backhaul, click a backhaul in this column.
	Shorthaul	Table column that lists the visible shorthauls. To access details for a specific shorthaul, click a shorthaul in this column. Note The graph shows a maximum of 12 shorthauls by default. To change the number of visible shorthauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Average	Table column that shows the average bits per second for the shorthaul.
	Minimum	Table column that shows the minimum number of bits per second for the shorthaul.
	Minimum Timestamp	Table column that shows time when the minimum bits-per-second value occurred.
	Maximum	Table column that shows maximum number of bits per second for the shorthaul.
	Maximum Timestamp	Table column that shows time when the maximum bits-per-second value occurred.
	Expand to Full Screen	Click this link to open the graph in a full-screen window for better viewing.
	Minimum Bits/Sec	Y-axis labels for graphs that show minimum, average, and maximum bits per second for the visible shorthauls.
	Average Bits/Sec	Note The graph shows a maximum of 12 shorthauls by default. To change the number of visible shorthauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Maximum Bits/Sec	
	<i>Legend</i>	Positioned below each graph, a legend of color-coded labels for each shorthaul that appears in the graph.
Table, CSV	Node	Table column that lists all the nodes that contain RAN backhauls. If Output is Table, to access details for a specific node, click a node in this column.
	Backhaul	Table column that lists all the RAN backhauls in the network. If Output is Table, to access details for a specific backhaul, click a backhaul in this column.
	Shorthaul	Table column that lists all the RAN shorthauls in the network. If Output is Table, to access details for a specific shorthaul, click a shorthaul in this column.
	Protocol	Table column that shows whether the shorthaul protocol is GSM or UMTS.
	Send	Table columns that show minimum, average, and maximum values and their timestamps for send traffic on the shorthaul.
	Receive	Table columns that show minimum, average, and maximum values and their timestamps for receive traffic on the shorthaul.

GSM Errors Daily

Output	GUI Element	Description
Graph	Node	Table column that lists nodes that contain GSM shorthauls. To access details for a specific node, click a node in this column.
	Backhaul	Table column that lists backhauls that contain GSM shorthauls. To access details for a specific backhaul, click a backhaul in this column.
	Shorthaul	Table column that lists the visible GSM shorthauls. To access details for a specific shorthaul, click a shorthaul in this column. Note The table shows a maximum of 12 shorthauls by default. To change the number of visible shorthauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Total Counts	Table column that lists the total number of GSM errors for the visible shorthauls during the chosen duration.
	Avg. Error Rate (Per Sec)	Table column that lists the average error rate each second for the visible shorthauls.
	Expand to Full Screen	Click this link to open the graph in a full-screen window for better viewing.
	Error Counts	Y-axis label for graph that shows total GSM errors for the visible GSM shorthauls. Note The graph shows a maximum of 12 shorthauls by default. To change the number of visible shorthauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	<i>Legend</i>	Positioned below the graph, a legend of color-coded labels for each shorthaul that appears in the graph.
Table, CSV	Node	Table column that lists all the nodes that contain GSM shorthauls. If Output is Table, to access details for a specific node, click a node in this column.
	Backhaul	Table column that lists all the backhauls that contain GSM shorthauls. If Output is Table, to access details for a specific backhaul, click a backhaul in this column.
	Shorthaul	Table column that lists all the GSM shorthauls in the network. If Output is Table, to access details for a specific shorthaul, click a shorthaul in this column.
	Total Errors	Table column that lists the total number of GSM errors for the visible shorthauls during the chosen duration.
	Total Missed Packets	Total number of missed packets on the GSM shorthaul.
	Total Protocol Errors	Total number of protocol errors on the GSM shorthaul.
	Total Miscellaneous Errors	Total number of miscellaneous errors on the GSM shorthaul.

UMTS Errors Daily

Output	GUI Element	Description
Graph	Node	Table column that lists nodes that contain UMTS shorthauls. To access details for a specific node, click a node in this column.
	Backhaul	Table column that lists backhauls that contain UMTS shorthauls. To access details for a specific backhaul, click a backhaul in this column.
	Shorthaul	Table column that lists the visible UMTS shorthauls. To access details for a specific shorthaul, click a shorthaul in this column. Note The table shows only 12 shorthauls by default. To change the number of visible shorthauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	Total Counts	Table column that lists the total number of UMTS errors that occurred for the visible shorthauls during the chosen duration.
	Avg. Error Rate (Per Sec)	Table column that lists the average error rate each second for the visible shorthauls during the chosen duration.
	Expand to Full Screen	Click this link to open the graph in a full-screen window for better viewing.
	Error Counts	Y-axis label for the graph that shows the total number of UMTS errors for the visible UMTS shorthauls. Note The graph shows only 12 shorthauls by default. To change the number of visible shorthauls, use the Graph Series Editor. See Using the Toolbar, page 11-5 , for more information.
	<i>Legend</i>	Positioned below the graph, a legend of color-coded labels for each UMTS shorthaul that appears in the graph.
Table, CSV	Node	Table column that lists nodes that contain UMTS shorthauls. If Output is Table, to access details for a specific node, click a node in this column.
	Backhaul	Table column that lists all the backhauls that contain UMTS shorthauls. If Output is Table, to access details for a specific backhaul, click a backhaul in this column.
	Shorthaul	Table column that lists all the UMTS shorthauls in the network. If Output is Table, to access details for a specific shorthaul, click a shorthaul in this column.
	Timestamp	Time that the error values occurred for the visible shorthauls.
	Total Errors	Table column that lists the total number of UMTS errors for the visible shorthauls during the chosen duration.
	Total Protocol Errors	Table column that lists the total number of protocol errors on the UMTS shorthaul.
	Total Miscellaneous Errors	Table column that lists the total number of miscellaneous errors on the UMTS shorthaul.

Viewing Accounting Reports

You can view any of the following statistics reports:

- [GTT Accounting Reports, page 12-41](#)
- [MTP3 Accounting Reports, page 12-42](#)
- [AS/ASP Accounting Reports, page 12-44](#)

GTT Accounting Reports

You can view summary reports of daily GTT accounting statistics. You can also export the reports.

GTT Accounting Statistics Daily Summary Reports

You can view a daily summary of GTT accounting statistics for all nodes that the MWTM detected on a specified date. The GTT Accounting Daily Report page shows all MWTM daily GTT accounting statistics detail reports by date. Each file contains a daily summary of GTT accounting statistics for all nodes that the MWTM detected on a specified date.

The GTT Accounting Daily Report table is sorted based on the information in the Packets column. However, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).



Note

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node associated with the From Network Name for which data is visible.
From Network Name	Name of the network from which GTT traffic originated, and for which data is visible.
Signaling Point	Name of the signaling point associated with the From Network Name instance for which data is visible.
Linkset	Name of the linkset associated with the From Network Name instance for which data is visible.
Selector	Name of the selector.
GTA	Global Title Address (GTA) associated with the selector.

Field or Column	Description
To Network Name	Name of the network in which the translated point code resides for GTT files, version: 4.1—Corresponds to ITP software release 12.2(20)SW or greater 4.2—Corresponds to ITP software release 12.2(21)SW1 or greater 4.3—Corresponds to ITP software release 12.2(25)SW1, 12.2(18)IXA, or 12.4(11)SW or higher 4.4—Corresponds to ITP software release 12.2(18)IXE or 12.4(15)SW or higher The value of this field is identical to that of the From Network Name field for GTT files, version: 3.1 (corresponding to ITP software releases 12.2(4)MB9 and 12.2(4)MB9a) 4.0 (corresponding to ITP software release 12.2(4)MB10 or greater)
Point Code	Destination point code for the GTA.
Packets	Total number of packets translated by GTT on the specified date.
Octets	Total number of octets translated by GTT on the specified date.

MTP3 Accounting Reports

You can view a daily summary of MTP3 accounting statistics for the MWTM on a specified date. You can also export the reports. MTP3 accounting describes MTP3 layer traffic in support of linksets. To enable MTP3 accounting reports, use the **mwtm statreps acct** command (see [mwtm statreps acct](#), page B-117).

This section covers:

- [MTP3 Accounting Statistics Daily Detail Reports](#), page 12-42
- [Daily MTP3/AS Accounting Statistics Archived Reports](#), page 12-44



Note

Every five minutes (by default), the ITP moves data records from a quick-access table to a database that stores long term accounting records. This database contains accumulated accounting data since the last clearing or from the time accounting was originally enabled. The MWTM shows only the data from this database, not from the quick-access table.

MTP3 Accounting Statistics Daily Detail Reports

You can view a daily summary of MTP3 accounting statistics for the MWTM on a specified date. The MTP3 Accounting Daily Report page shows detail reports of all MWTM daily MTP3 accounting statistics by date. Each file contains a daily summary of MTP3 accounting statistics for the MWTM on a specified date.

The MTP3 Accounting Daily Report table is sorted based on the information in the Send MSUs column. However, you can sort the table based on the information in one of the other columns (see [Navigating Table Columns](#), page 5-24).

**Note**

If you do not enable data collection on the active report, a red ball  and the words `Data Collection Disabled` appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then `MathError` appears in the field.

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the linkset.
Network Name	Name of the network for the linkset.
Signaling Point	Name of the signaling point for the linkset.
Linkset	Name of the linkset.
Gateway Screening	Indicates whether the traffic passed or failed the Gateway Screening test at the ITP. To see only statistics that passed or failed for a specific linkset, select a linkset and click Pass , Fail , or Unroutable .
OPC	Originating point code of the traffic, which is a unique identifier for each set of statistics. To see only statistics that match a specific OPC for a given linkset, find the linkset and click the point code.
DPC	Destination point code of the traffic. To see only statistics that match a specific DPC for a given linkset, find the linkset and click the point code.
SI	Service indicator, which indicates the type of SS7 traffic. Valid values include: • 0—Signaling Network Management Message (SNM) • 1—Maintenance Regular Message (MTN) • 2—Maintenance Special Message (MTNS) • 3—Signaling Connection Control Part (SCCP) • 4—Telephone User Part (TUP) • 5—ISDN User Part (ISUP) • 6—Data User Part (call and circuit-related messages) • 7—Data User Part (facility registration/cancellation messages) To see only more information for a specific type of SI, click the SI type.
Send MSUs	Total number of MTP3 MSUs sent on the specified date.
Receive MSUs	Total number of MTP3 MSUs received on the specified date.
Send Bytes	Total number of bytes sent on the specified date.
Receive Bytes	Total number of bytes received on the specified date.

Daily MTP3/AS Accounting Statistics Archived Reports

The MTP3/AS Daily Archived Accounting Reports page shows all archived MWTM daily MTP3/AS accounting statistics reports for the server to which you connect, stored as downloadable *.zip* files.

The *.zip* files are archived by date; for example, the *sgmAccStats.DailyDetail.2007-02-13.csv.zip* file contains the daily MTP3 accounting statistics report for February 13, 2007.



Note

To limit the maximum number of rows in export CSV files (for example, Excel can only handle about 65535 rows.) See [mwtm statreps maxcsvrows](#), page B-123.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a daily MTP3 accounting statistics report for that date. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about accounting statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

AS/ASP Accounting Reports

You can view daily reports for application server (AS) and application server process (ASP) accounting statistics by using the MWTM. You can also export the report. AS/ASP accounting describes MTP3 layer traffic in support of application servers. To enable AS/ASP accounting reports, use the ***mwtm statreps acct*** command (see [mwtm statreps acct](#), page B-117).

Field or Column	Description
Date	Date of the report.
Node	Name of the node for the linkset.
Network Name	Name of the network for the linkset.
Signaling Point	Name of the signaling point for the linkset.
AS	Name of the application server.
OPC	Originating point code of the traffic, which is a unique identifier for each set of statistics. To see only statistics that match a specific OPC for a given linkset, find the linkset and click the point code.
DPC	Destination point code of the traffic. To see only statistics that match a specific DPC for a given linkset, find the linkset and click the point code.

Field or Column	Description
SI	Service indicator, which indicates the type of Signaling System 7 (SS7) traffic. Valid values include: • 0—Signaling Network Management Message (SNM) • 1—Maintenance Regular Message (MTN) • 2—Maintenance Special Message (MTNS) • 3—Signaling Connection Control Part (SCCP) • 4—Telephone User Part (TUP) • 5—ISDN User Part (ISUP) • 6—Data User Part (call and circuit-related messages) • 7—Data User Part (facility registration/cancellation messages) To see only more information for a specific type of SI, click the SI type.
Send MSUs	Total number of MTP3 MSUs sent on the specified date.
Receive MSUs	Total number of MTP3 MSUs received on the specified date.
Send Bytes	Total number of bytes sent on the specified date.
Receive Bytes	Total number of bytes received on the specified date.

Viewing File Archive Reports

Reports that have been archived are located within File Archive > Reports in the MWTM web interface. All archived reports are saved as export files in .csv format.

You can view any of the following archived reports:

- [Custom Archived Reports, page 12-46](#)
- [Daily Archived Reports, page 12-48](#)
- [Hourly Archived Reports, page 12-49](#)
- [Rolling Archived Reports, page 12-49](#)
- [Application Server Archived Reports, page 12-50](#)
- [Application Server Process Archived Reports, page 12-50](#)
- [GTT Accounting Archived Reports, page 12-51](#)
- [Link Archived Reports, page 12-52](#)
- [Linkset Archived Reports, page 12-52](#)
- [MLR Archived Reports, page 12-53](#)
- [MSU Archived Reports, page 12-54](#)
- [MTP3/AS Archived Reports, page 12-55](#)
- [Point Codes Archived Reports, page 12-58](#)
- [Q.752 Hourly Archived Reports, page 12-58](#)

You can also view MWTM statistics reports logs (see [Viewing the MWTM Statistics Reports Logs, page 12-59](#)).

Custom Archived Reports

The Custom Archived Report pages show all archived MWTM custom network and accounting statistics reports for the server to which you connect. These reports can be viewed on the Web, or downloaded as .zip files. These .zip files are also stored in the default directory (/opt/CSCOs_{sgm} by default) in the /reports/custom directory.


Note

Custom (and hourly) Q.752 reports are only available as .zip files.

Custom archived reports are those that you enable by using these commands:

Command	Generates these custom statistics:
mwtm accstats	Accounting
mwtm ggsnstats	GGSN
mwtm gttstats	GTT
mwtm linkstats	Link and linkset
mwtm mlrstats	MLR
mwtm msustats	MSU rates
mwtm mtpevents	MTP event
mwtm q752stats	Q.752
mwtm xuastats	Application server and application server process


Note

For detailed descriptions of these commands, see [Appendix B, “Command Reference.”](#)

The Custom Report tables are sorted based on the information in the Export File column. However, you can sort a table based on the information in one of the other columns (see [Navigating Table Columns, page 5-24](#)).

The Custom Report tables contain:

Column	Description
Export File	Name of the custom statistics export .zip file, archived by type, date, and hour; for example, the <i>sgmLinksetStats.custom.20867.2007-02-13-16:15.csv.zip</i> file contains the summary report of custom linkset statistics with the ID tag 20867 for the 15th minute of the 16th hour on February 13, 2007. Each archived .zip file contains a comma-separated value (CSV) text file with a daily statistics report for that date. You can download the .zip files and extract them. To download a .zip file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel. For details about custom statistics archived reports, see: ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt.
Report Start Date (EST)	Date and time the custom report began.

Column	Description
Report Finish Date (EST)	Date and time the custom report ended.
Last Modified Date (EST)	Date and time the custom report was last modified.
View	Shows the custom detail report for the object. Not available for Q.752 reports.

To show details in HTML for custom archived reports, click on a link in the View column of the Custom Archived Report page:

Link	Description
Aborts and Continues	Daily MLR Aborts Reports, page 12-27 Daily MLR Continues Reports, page 12-28
Application Servers	Hourly Application Server Reports, page 12-9
Application Server Processes	Hourly Application Server Process Reports, page 12-12
Events	Custom MTP3 Events Detail Reports, page 12-57
GTT	GTT Accounting Statistics Daily Summary Reports, page 12-41
Links	Hourly Link Reports, page 12-18
Linksets	Hourly Linkset Reports, page 12-23
Processed	Daily MLR Processed Reports, page 12-29
ResultInvokes	Daily MLR Result Invokes Reports, page 12-30
RuleMatches	Daily MLR RuleMatches Reports, page 12-31
SubTriggers	Daily MLR SubTriggers Reports, page 12-31
Triggers	Daily MLR Triggers Reports, page 12-32

All custom detail reports contain these headings and general menu options:

Heading/ Menu Option	Description
Date and Hour (in heading)	Date and hour of the report.
Offset (in heading)	Shows the number of rows in the table, prior to the first visible row; for example, if the first visible row is 501, the Offset is 500.
Number and Sort Order (in heading)	Shows the number of records (rows) in the table, the column by which the table is sorted, and whether the sort is in ascending or descending order.
10/Page	Shows 10 rows in the table.
20/Page	Shows 20 rows in the table.
50/Page	Shows 50 rows in the table.

Heading/ Menu Option	Description
100/Page	Shows 100 rows in the table.
300/Page	Shows 300 rows in the table.
500/Page	Shows 500 rows in the table.
Max	Shows up to 15,000 rows in the table. Note Depending on the number of rows, this could take up to 15 minutes.
DefPrefs	Resets the /Page preferences for this web page to the default settings for the MWTM server.
First (at bottom of table)	Shows the first page of entries for the table. For example, if the table is sorted by Total Aborted in descending order, clicking this field shows the entries with the highest number of MSUs aborted by MLR. You cannot click this field if the first page of entries is already visible.
Previous (Rows) (at bottom of table)	Shows the previous page of entries for the table. You cannot click this field if the first page of entries is already visible.
Next (Rows) (at bottom of table)	Shows the next page of entries for the table. You cannot click this field if the last page of entries is already visible.
Last (at bottom of table)	Shows the last page of entries for the table. For example, if the table is sorted by Total Aborted in descending order, clicking this field shows the entries with the lowest number of MSUs aborted by MLR. You cannot click this field if the last page of entries is already visible.
Total (at bottom of table)	Shows the total number of entries in the table.

Daily Archived Reports

The Daily Archived Reports pages display summary reports for all archived MWTM daily network statistics for all application servers, application server processes, links, linksets, MLR, or point codes that the MWTM detects for the server to which you connect, stored as downloadable .zip files.

The .zip files are archived by type and hour; for example, the *sgmLinksetStats.DailySum.2007-02-13.csv.zip* file contains the summary report of daily linkset statistics for the February 13, 2007.

Each archived .zip file contains a comma-separated value (CSV) text file with a summary report of daily network statistics for all application servers, application server processes, links, linksets, MLR, or point codes that the MWTM detected on that date and hour. You can download the .zip files and extract them.

To download a .zip file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about daily network statistics archived reports, see:

<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Hourly Archived Reports

The Hourly Archived Reports pages show summary reports for all archived MWTM hourly network statistics for all of the following that the MWTM detects for the server to which you connect:

- Application servers
- Application server processes
- Links
- Linksets
- Q752 links

The summary reports of archived hourly network statistics are stored as downloadable *.zip* files. The *.zip* files are archived by type, date, and hour; for example, the *sgmLinksetStats.2007-02-13-08.csv.zip* file contains summary reports for the hourly linkset statistics for the eighth hour on February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of hourly network statistics for all application servers, application server processes, links, or linksets that the MWTM detects on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about the format of hourly network statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Rolling Archived Reports

The All Rolling Reports page shows summary reports of concatenated MWTM hourly and daily network statistics for all of the following objects detected by the MWTM for the server you are connected to:

- Application servers
- Application server processes
- Links
- Linksets

These statistics are stored as downloadable *.zip* files. The *.zip* files are archived by type and number of days (7 or 30). For example:

- The *sgmLinkStats.RollingSevenDayAllHours.csv.zip* file contains summary reports of the hourly link statistics for the last seven (7) days, concatenated into one comma-separated value (CSV) text file.
- The *sgmLinkStats.Rolling30DayAllDays.csv.zip* file contains summary reports of the daily link statistics for the last 30 days, concatenated into one comma-separated value (CSV) text file.

**Note**

To limit the maximum number of rows in export CSV files (for example, Excel can only handle 65,535 rows.) See [mwtm statreps maxcsvrows](#), page B-123.

The MWTM creates a new set of files every hour.

You can download the *.zip* files and extract them. To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about rolling statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Application Server Archived Reports

You can access these reports:

- [Daily Application Server Archived Reports, page 12-50](#)
- [Hourly Application Server Archived Reports, page 12-50](#)

**Note**

For details about custom application server archived reports, see [Custom Archived Reports, page 12-46](#).

Daily Application Server Archived Reports

The AS Daily Archived Reports page shows summary reports for all archived MWTM daily network statistics for all application servers that the MWTM detects for the server to which you connect. The information is stored as downloadable *.zip* files.

The *.zip* files are archived by type and date; for example, the *sgmASEStats.DailySum.2007-02-13.csv.zip* file contains the summary report for daily application server statistics for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of daily network statistics for all application servers that the MWTM detects on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about daily application server statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Hourly Application Server Archived Reports

The AS Hourly Archived Reports page shows all summary reports for archived MWTM hourly network statistics for all application servers that the MWTM detects for the server to which you connect. The information is stored as downloadable *.zip* files.

The *.zip* files are archived by type, date, and hour; for example, the *sgmASEStats.2007-02-13-08.csv.zip* file contains the summary report for hourly application server statistics for the 8th hour on February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of hourly network statistics for all application servers that the MWTM detected on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about hourly application server statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Application Server Process Archived Reports

You can access these reports:

- [Daily Application Server Process Archived Reports, page 12-51](#)
- [Daily Application Server Process Archived Reports, page 12-51](#)

**Note**

For details about custom application server archived reports, see [Custom Archived Reports, page 12-46](#).

Daily Application Server Process Archived Reports

The ASP Daily Archived Reports page shows summary reports of all archived MWTM daily network statistics for all application server processes that the MWTM detects for the server to which connect, stored as downloadable *.zip* files.

The *.zip* files are archived by type and date; for example, the *sgmASPStats.DailySum.2007-02-13.csv.zip* file contains the summary report of daily application server process statistics for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of daily network statistics for all application server processes that the MWTM detected on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, right-click a filename, then save the file to a location of your choice. You can also import the file into Microsoft Excel.

For details about daily application server process statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Hourly Application Server Process Archived Reports

The ASP Hourly Archived Reports page shows the summary reports of all archived MWTM hourly network statistics for all application server processes that the MWTM detects for the server to which you connect, stored as downloadable *.zip* files.

The *.zip* files are archived by type, date, and hour; for example, the *sgmASPStats.2007-02-13.csv.zip* file contains the summary report of hourly application server process statistics for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with the summary report for hourly network statistics for all application server processes that the MWTM detected on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about hourly application server process statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

GTT Accounting Archived Reports

You can access the daily GTT accounting statistics archived reports. For details about custom GTT accounting archived reports, see [Custom Archived Reports, page 12-46](#).

Daily GTT Accounting Statistics Archived Reports

The GTT Daily Archived Accounting Reports page shows all archived MWTM daily GTT accounting statistics reports for the server to which you connect, stored as downloadable *.zip* files.

The *.zip* files are archived by type and date; for example, the *sgmGTTStats.DailyDetail.2007-02-13.csv.zip* file contains the daily GTT accounting statistics report for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a daily GTT accounting statistics report for that date. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about GTT accounting statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Link Archived Reports

You can access these reports:

- [Hourly Link Statistics Archived Reports, page 12-52](#)
- [Daily Link Statistics Archived Reports, page 12-52](#)



Note

For details about custom link archived reports, see [Custom Archived Reports, page 12-46](#).

Hourly Link Statistics Archived Reports

The Link Hourly Archived Reports page shows summary reports for all archived MWTM hourly network statistics for all links that the MWTM detected for the server to which you connect, stored as downloadable *.zip* files.

The *.zip* files are archived by type, date, and hour; for example, the *sgmLinkStats.2007-02-13-09.csv.zip* file contains the summary reports for hourly link statistics for February 13, 2007 at 9:00am.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of an hourly network statistics for all links that the MWTM detected on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about hourly link statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Daily Link Statistics Archived Reports

The Link Daily Archived Reports page shows summary reports for all archived MWTM daily network statistics for all links that the MWTM detected for the server to which you connect, stored as downloadable *.zip* files.

The *.zip* files are archived by type and date; for example, the *sgmLinkStats.DailySum.2007-02-13.csv.zip* file contains the summary report of daily link statistics for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of daily network statistics for all links that the MWTM detected on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about daily link statistics archived reports, see:
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Linkset Archived Reports

You can access these reports:

- [Hourly Linkset Statistics Archived Reports, page 12-53](#)
- [Daily Linkset Statistics Archived Reports, page 12-53](#)

**Note**

For details about custom linkset archived reports, see [Custom Archived Reports, page 12-46](#).

Hourly Linkset Statistics Archived Reports

The Linkset Hourly Archived Reports page shows summary reports of all archived MWTM hourly network statistics for all linksets that the MWTM detects for the server to which you connect, stored as downloadable .zip files.

The .zip files are archived by type, date, and hour; for example, the *sgmLinksetStats.2007-02-13.csv.zip* file contains the summary report for the hourly linkset statistics for February 13, 2007.

Each archived .zip file contains a comma-separated value (CSV) text file with a summary report of hourly network statistics for all linksets that the MWTM detected on that date and hour. You can download the .zip files and extract them.

To download a .zip file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about hourly linkset statistics archived reports, see:

<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Daily Linkset Statistics Archived Reports

The Linkset Daily Archived Reports page shows the summary report of all archived MWTM daily network statistics for all linksets that the MWTM detected for the server to which you connect, stored as downloadable .zip files.

The .zip files are archived by type and date; for example, the *sgmLinksetStats.DailySum.2007-02-13.csv.zip* file contains the summary reports of daily linkset statistics for February 13, 2007.

Each archived .zip file contains a comma-separated value (CSV) text file with a summary report of daily network statistics for all linksets that the MWTM detected on that date and hour. You can download the .zip files and extract them.

To download a .zip file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about daily linkset statistics archived reports, see:

<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

MLR Archived Reports

**Note**

For details about custom MLR statistics archived reports, see [Custom Archived Reports, page 12-46](#).

The MLR Daily Archived Reports pages show all archived MWTM daily MLR processed, aborts, continues, result invokes, rule matches, subtriggers, and triggers statistics reports for the server to which you connect, stored as downloadable .zip files.

The *.zip* files are archived by type and date; for example, the:

- *mwtmMLRStats.DailyAbortCons.2007-02-13.csv.zip* file contains the daily MLR aborts and report for February 13, 2007.
- *mwtmMLRStats.DailyProcessed.2007-02-13.csv.zip* file contains the daily MLR processed report for February 13, 2007.
- *mwtmMLRStats.DailyResultInvokes.2007-02-13.csv.zip* file contains the daily MLR result invokes report for February 13, 2007.
- *mwtmMLRStats.DailyRuleMatches.2007-02-13.csv.zip* file contains the daily MLR rule matches report for February 13, 2007.
- *mwtmMLRStats.DailySubTriggers.2007-02-13.csv.zip* file contains the daily MLR subtriggers report for February 13, 2007.
- *mwtmMLRStats.DailyTriggers.2007-02-13.csv.zip* file contains the daily MLR triggers report for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a daily MLR statistics report for that date. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about MLR statistics archived reports, see:

<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

MSU Archived Reports

You can access these reports:

- [Hourly MSU Archived Reports, page 12-54](#)
- [Daily MSU Archived Reports, page 12-55](#)



Note

For details about custom MSU archived reports, see [Custom Archived Reports, page 12-46](#).

Hourly MSU Archived Reports

The MSU Hourly Archived Reports page shows summary reports of all archived MWTM hourly MSU rates that the MWTM detects for the server to which you connect, stored as downloadable *.zip* files.

The *.zip* files are archived by type, date, and hour; for example, the *itpHourlyMsuLoad.2007-02-13.csv.zip* file contains the summary report for the hourly MSU rates for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of hourly MSU rates that the MWTM detected on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about hourly MSU archived reports, see:

<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Daily MSU Archived Reports

The MSU Daily Archived Reports page shows the summary report of all archived MWTM daily MSU rates that the MWTM detected for the server to which you connect, stored as downloadable .zip files.

The .zip files are archived by type and date; for example, the *itpDailyMsuLoad.2007-02-13.csv.zip* file contains the summary reports of daily MSU rates for February 13, 2007.

Each archived .zip file contains a comma-separated value (CSV) text file with a summary report of daily MSU rates that the MWTM detected on that date and hour. You can download the .zip files and extract them.

To download a .zip file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about daily MSU archived reports, see:

<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

MTP3/AS Archived Reports

You can access these reports:

- [MTP3 Event Reports, page 12-55](#)
- [Custom MTP3 Events Detail Reports, page 12-57](#)
- [Custom MTP3/AS Accounting Detail Reports, page 12-57](#)

MTP3 Event Reports

This section contains:

- [Hourly MTP3/AS Event Reports, page 12-55](#)
- [Custom MTP3/AS Event Reports, page 12-56](#)

Hourly MTP3/AS Event Reports

To create hourly MTP3/AS event reports for the MWTM:

Step 1 Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).

Step 2 Enter these commands:

```
# cd /opt/CSC0sgm/bin
# ./mwtm evreps enable
# ./mwtm evreps mtp
```

For more details on the **mwtm evreps** commands, see [Appendix B, “Command Reference.”](#)

The MTP3/AS Hourly Events Archived Reports page shows all hourly MWTM MTP3/AS event reports for the server to which you connect.

The .zip files are archived by type, date, and hour; for example, the *sgmMTP3Events.2006-06-29-08.csv.zip* file contains a summary report of the hourly MTP3 event for the eighth hour on June 29, 2006.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of an hourly MTP3 event for all objects that the MWTM detected on that date and hour. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about hourly MTP3 event reports, see
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

Custom MTP3/AS Event Reports

To create custom MTP3/AS event reports for the MWTM:

-
- Step 1** Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).
- Step 2** Enter these commands:
- ```
cd /opt/CSC0sgm/bin
./mwtm mtpevents
```

For more details on the **mwtm mtpevents** command, see [Appendix B, “Command Reference.”](#)

---

The Custom MTP3/AS Events Archived Reports page shows all custom MWTM MTP3/AS event reports for the server to which you connect.

| Field or Column          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Export File              | <p>Name of the custom network events export <i>.zip</i> file, archived by type, date, and hour; for example, the <i>sgmMTP3Events.custom.20867.2006-02-13-16-15.csv.zip</i> file contains the summary report of custom network events with ID tag 20867 for the 15th minute of the 16th hour on February 13, 2006.</p> <p>Each archived <i>.zip</i> file contains a comma-separated value (CSV) text file with a daily statistics report for that date. You can download the <i>.zip</i> files and extract them.</p> <p>To download a <i>.zip</i> file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.</p> <p>For details about custom statistics archived reports, see:<br/> <a href="ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt">ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt</a>.</p> |
| Report Start Date (EST)  | Date and time the custom report began.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Report Finish Date (EST) | Date and time the custom report ended.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Last Modified Date (EST) | Date and time the custom report was last modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| View                     | Shows the custom detail report for the object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Custom MTP3 Events Detail Reports

The Custom MTP3 Events Detail Reports page shows details for all archived MWTM custom MTP3 event reports for all nodes that the MWTM detected when you enabled the report. You enable Custom event reports by using the **mwtm mtpevents** command.

| Field or Column | Description                                                                                                                                                                                           |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID              | Identifier for the custom report, specified when you entered the <b>mwtm mtpevents</b> command. If you did not specify an ID, this field shows the process ID of the command that enabled the report. |
| Node            | Name of the node.                                                                                                                                                                                     |
| Index           | Number in the list shown in the CLI.                                                                                                                                                                  |
| MTP3 Event Text | MTP3 event message as seen on the CLI.                                                                                                                                                                |

## Custom MTP3/AS Accounting Detail Reports

The Custom MTP3/AS Accounting Detail Reports page shows a custom summary of MTP3/AS accounting statistics for links and linksets in the MWTM. Custom MTP3/AS accounting reports are enabled using the **mwtm accstats** command.



### Note

If you do not enable data collection on the active report, a red ball  and the words *Data Collection Disabled* appear next to the report title. Click the **Data Collection Disabled** link to see which command enables the report.

If a statistics calculation results in an undefined value, such as a number divided by zero (0), or an undefined number, based on the configuration, then *MathError* appears in the field.

| Field or Column   | Description                                                                                                                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID                | Internal ID, assigned by the MWTM, of the chosen hourly accounting statistics report.<br><br>To see the entire detailed report, click the ID. The MWTM shows the Accounting Data Record # X for Date for that date and hour, in text format. The Accounting Data Record # X for Date can be useful when the TAC is debugging problems. |
| Node              | Name of the node for the linkset.                                                                                                                                                                                                                                                                                                      |
| Network Name      | Name of the network for the linkset.                                                                                                                                                                                                                                                                                                   |
| Sig Point         | Name of the signaling point for the linkset.                                                                                                                                                                                                                                                                                           |
| Linkset           | Name of the linkset.                                                                                                                                                                                                                                                                                                                   |
| Gateway Screening | Indicates whether the traffic passed or failed the Gateway Screening test at the ITP.<br><br>To see only statistics that passed or failed for a specific linkset, select a linkset and click <b>Pass</b> , <b>Fail</b> , or <b>Unroutable</b> .                                                                                        |

| Field or Column | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OPC             | Originating point code of the traffic, which is a unique identifier for each set of statistics.<br><br>To see only statistics that match a specific OPC for a given linkset, find the linkset and click the point code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| DPC             | Destination point code of the traffic.<br><br>To see only statistics that match a specific DPC for a given linkset, find the linkset and click the point code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SI              | Service indicator, which indicates the type of SS7 traffic. Valid values include: <ul style="list-style-type: none"> <li>• <b>0</b>—Signaling Network Management Message (SNM)</li> <li>• <b>1</b>—Maintenance Regular Message (MTN)</li> <li>• <b>2</b>—Maintenance Special Message (MTNS)</li> <li>• <b>3</b>—Signaling Connection Control Part (SCCP)</li> <li>• <b>4</b>—Telephone User Part (TUP)</li> <li>• <b>5</b>—ISDN User Part (ISUP)</li> <li>• <b>6</b>—Data User Part (call and circuit-related messages)</li> <li>• <b>7</b>—Data User Part (facility registration/cancellation messages)</li> </ul> To see only detailed information for a specific type of SI, click the SI type. |
| Send MSUs       | Total number of MTP3 MSUs sent on the specified date.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Receive MSUs    | Total number of MTP3 MSUs received on the specified date.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Send Bytes      | Total number of bytes sent on the specified date.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Receive Bytes   | Total number of bytes received on the specified date.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Point Codes Archived Reports

The Point Codes Daily Archived Reports page shows all archived MWTM daily point code inventory reports for the server to which you connect, stored as downloadable *.zip* files.

On the Point Codes Daily Archived Reports page, the *.zip* files are archived by date; for example, the *sgmPointCodes.DailyInv.2007-02-13.csv.zip* file contains the daily point code inventory report for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a list of all point codes that were being used by all nodes that the MWTM detected on that date. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about point code inventory archived reports, see:  
<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

## Q.752 Hourly Archived Reports

The Q752 Hourly Archived Reports page shows all archived MWTM hourly Q.752 reports for the server to which you connect, stored as downloadable *.zip* files.

On the Q752 Hourly Archived Reports page, the *.zip* files are archived by date; for example, the *sgmQ752Stats.2007-02-13.csv.zip* file contains the hourly Q.752 report for February 13, 2007.

Each archived *.zip* file contains a comma-separated value (CSV) text file with a summary report of all Q.752 links that the MWTM detected on that date. You can download the *.zip* files and extract them.

To download a *.zip* file, click a filename, then save the file to a location of your choice. You can also import the file directly into Microsoft Excel.

For details about Q.752 hourly archived reports, see:

<ftp://ftp-eng.cisco.com/ftp/mwtm/docs/README-ExportReports.txt>.

## Viewing the MWTM Statistics Reports Logs

You can view a log that contains all messages pertaining to MWTM reports, and a display of the current values of MWTM report parameters and timers.

This section contains this information:

- [Viewing the MWTM Report Log, page 12-59](#)
- [For details on viewing the MWTM report log, see Viewing the Report Log, page 11-25., page 12-59](#)

## Viewing the MWTM Report Log

For details on viewing the MWTM report log, see [Viewing the Report Log, page 11-25](#).

## Viewing the MWTM Report Parameters and Timers

The Report Parameters and Timers page shows the current values of report parameters and timers for the server to which you connect, and which is currently running the MWTM server.

To access the Report Parameters and Timers page:

- 
- Step 1** Choose **Reports** from the MWTM web navigation tree.
- Step 2** Click the **Report Parameters & Timers** button in the toolbar.
- 

| Column        | Description                                                                                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Report Dir    | Path and name of the directory in which the MWTM stores reports. The default reports directory is <i>/opt/CSCOsgm/reports</i> , but you can change the reports directory using the <b>mwtm repdir</b> command (see <a href="#">mwtm repdir, page B-112</a> ). |
| Status        | Indicates whether the MWTM should generate network statistics reports. For more information, see the description of the <b>mwtm statreps [disable   enable]</b> command in <a href="#">mwtm statreps servratio, page B-126</a> .                              |
| ExportReports | Indicates whether the MWTM should generate network statistics reports in export format. For more information, see the description of the <b>mwtm statreps [export   noexport]</b> command in <a href="#">mwtm statreps export, page B-120</a> .               |
| LinkReports   | Indicates whether the MWTM should generate summary reports of link and linkset statistics. For more information, see the description of the <b>mwtm statreps [link   nolink]</b> command in <a href="#">mwtm statreps link, page B-122</a> .                  |

| Column      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AcctReports | Indicates whether the MWTM should generate MTP3 accounting statistics reports. For more information, see the description of the <b>mwtm statreps [acct   noacct]</b> command in <a href="#">mwtm statreps acct</a> , page B-117.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| GTTReports  | Indicates whether the MWTM should generate GTT accounting statistics reports. For more information, see the description of the <b>mwtm statreps [gtt   nogtt]</b> command in <a href="#">mwtm statreps gtt</a> , page B-121.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| MLRReports  | Indicates whether the MWTM should generate MLR statistics reports. For more information, see the description of the <b>mwtm statreps [mlr   nomlr]</b> command in <a href="#">mwtm statreps mlr</a> , page B-123.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| XUARports   | Indicates whether the MWTM should generate accounting statistics reports for application servers and application server processes. For more information, see the description of the <b>mwtm statreps [xua   noxua]</b> command in <a href="#">mwtm statreps xua</a> , page B-128.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| MSUReports  | Indicates whether the MWTM should generate MSU rates reports. For more information, see the description of the <b>mwtm statreps [msu   nomsu]</b> command in <a href="#">mwtm statreps msu</a> , page B-124.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| IPLinks     | Indicates whether the MWTM should include links that use the Stream Control Transmission Protocol (SCTP) IP transport protocol in network statistics reports. For more information, see the description of the <b>mwtm statreps [iplinks   noiplinks]</b> command in <a href="#">mwtm statreps iplinks</a> , page B-122.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Q752Reports | Indicates whether the MWTM should generate Q.752 reports. For more information, see the description of the <b>mwtm statreps [q752   noq752]</b> command in <a href="#">mwtm statreps q752</a> , page B-125.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| NullCaps    | Indicates whether the MWTM should include SCTP links that do not have planned send and receive capacities in network statistics reports. For more information, see the description of the <b>mwtm statreps [nullcaps   nonullcaps]</b> command in <a href="#">mwtm statreps nullcaps</a> , page B-125.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| TimeMode    | Indicates the time mode for dates in network statistics reports. For more information, see the description of the <b>mwtm statreps timemode [12   24]</b> command in <a href="#">mwtm statreps timemode</a> , page B-127.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DiskCheck   | Indicates whether the MWTM should verify that a disk has at least 10 MB of space remaining before enabling network statistics reports. For more information, see the description of the <b>mwtm statreps [diskcheck   nodiskcheck]</b> command in <a href="#">mwtm statreps diskcheck</a> , page B-119.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| UtilRatio   | <p>Utilization values that are outside a normal range are indicated with a red status ball icon in the Send Utilization or Receive Utilization cell. A Utilization value is outside the normal range if the following condition is met:</p> <p style="text-align: center;"><b>Current Utilization &gt; factor * Long-Term Utilization</b></p> <p>This inequality is used to recognize increases in the Utilization value. Assuming the default factor of 1.5, the Current Utilization value must be less than or equal to 150% of the Long-Term Utilization value to be in the normal range.</p> <p>The default value for <i>factor</i> is <b>1.5</b>.</p> <p>For more information, see the description of the <b>mwtm statreps utilratio</b> command in <a href="#">mwtm statreps utilratio</a>, page B-128.</p> |



| Column      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GTTReports  | Indicates whether the MWTM should generate GTT accounting statistics reports. For more information, see the description of the <b>mwtm statreps [gtt   nogtt]</b> command in <a href="#">mwtm statreps gtt</a> , page B-121.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MLRReports  | Indicates whether the MWTM should generate MLR statistics reports. For more information, see the description of the <b>mwtm statreps [mlr   nomlr]</b> command in <a href="#">mwtm statreps mlr</a> , page B-123.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| XUARports   | Indicates whether the MWTM should generate accounting statistics reports for application servers and application server processes. For more information, see the description of the <b>mwtm statreps [xua   noxua]</b> command in <a href="#">mwtm statreps xua</a> , page B-128.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MSUReports  | Indicates whether the MWTM should generate MSU rates reports. For more information, see the description of the <b>mwtm statreps [msu   nomsu]</b> command in <a href="#">mwtm statreps msu</a> , page B-124.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IPLinks     | Indicates whether the MWTM should include links that use the Stream Control Transmission Protocol (SCTP) IP transport protocol in network statistics reports. For more information, see the description of the <b>mwtm statreps [iplinks   noiplinks]</b> command in <a href="#">mwtm statreps iplinks</a> , page B-122.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Q752Reports | Indicates whether the MWTM should generate Q.752 reports. For more information, see the description of the <b>mwtm statreps [q752   noq752]</b> command in <a href="#">mwtm statreps q752</a> , page B-125.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| NullCaps    | Indicates whether the MWTM should include SCTP links that do not have planned send and receive capacities in network statistics reports. For more information, see the description of the <b>mwtm statreps [nullcaps   nonullcaps]</b> command in <a href="#">mwtm statreps nullcaps</a> , page B-125.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| TimeMode    | Indicates the time mode for dates in network statistics reports. For more information, see the description of the <b>mwtm statreps timemode [12   24]</b> command in <a href="#">mwtm statreps timemode</a> , page B-127.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| DiskCheck   | Indicates whether the MWTM should verify that a disk has at least 10 MB of space remaining before enabling network statistics reports. For more information, see the description of the <b>mwtm statreps [diskcheck   nodiskcheck]</b> command in <a href="#">mwtm statreps diskcheck</a> , page B-119.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| UtilRatio   | <p>Utilization values that are outside a normal range are indicated with a red status ball icon in the Send Utilization or Receive Utilization cell. A Utilization value is outside the normal range if the following condition is met:</p> $\text{Current Utilization} > \text{factor} * \text{Long-Term Utilization}$ <p>This inequality is used to recognize increases in the Utilization value. Assuming the default factor of 1.5, the Current Utilization value must be less than or equal to 150% of the Long-Term Utilization value to be in the normal range.</p> <p>The default value for <i>factor</i> is <b>1.5</b>.</p> <p>For more information, see the description of the <b>mwtm statreps utilratio</b> command in <a href="#">mwtm statreps utilratio</a>, page B-128.</p> |

| Column      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GTTReports  | Indicates whether the MWTM should generate GTT accounting statistics reports. For more information, see the description of the <b>mwtm statreps [gtt   nogtt]</b> command in <a href="#">mwtm statreps gtt</a> , page B-121.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| MLRReports  | Indicates whether the MWTM should generate MLR statistics reports. For more information, see the description of the <b>mwtm statreps [mlr   nomlr]</b> command in <a href="#">mwtm statreps mlr</a> , page B-123.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| XUARReports | Indicates whether the MWTM should generate accounting statistics reports for application servers and application server processes. For more information, see the description of the <b>mwtm statreps [xua   noxua]</b> command in <a href="#">mwtm statreps xua</a> , page B-128.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| MSUReports  | Indicates whether the MWTM should generate MSU rates reports. For more information, see the description of the <b>mwtm statreps [msu   nomsu]</b> command in <a href="#">mwtm statreps msu</a> , page B-124.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IPLinks     | Indicates whether the MWTM should include links that use the Stream Control Transmission Protocol (SCTP) IP transport protocol in network statistics reports. For more information, see the description of the <b>mwtm statreps [iplinks   noiplinks]</b> command in <a href="#">mwtm statreps iplinks</a> , page B-122.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Q752Reports | Indicates whether the MWTM should generate Q.752 reports. For more information, see the description of the <b>mwtm statreps [q752   noq752]</b> command in <a href="#">mwtm statreps q752</a> , page B-125.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| NullCaps    | Indicates whether the MWTM should include SCTP links that do not have planned send and receive capacities in network statistics reports. For more information, see the description of the <b>mwtm statreps [nullcaps   nonullcaps]</b> command in <a href="#">mwtm statreps nullcaps</a> , page B-125.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| TimeMode    | Indicates the time mode for dates in network statistics reports. For more information, see the description of the <b>mwtm statreps timemode [12   24]</b> command in <a href="#">mwtm statreps timemode</a> , page B-127.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| DiskCheck   | Indicates whether the MWTM should verify that a disk has at least 10 MB of space remaining before enabling network statistics reports. For more information, see the description of the <b>mwtm statreps [diskcheck   nodiskcheck]</b> command in <a href="#">mwtm statreps diskcheck</a> , page B-119.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| UtilRatio   | <p>Utilization values that are outside a normal range are indicated with a red status ball icon in the Send Utilization or Receive Utilization cell. A Utilization value is outside the normal range if the following condition is met:</p> $\text{Current Utilization} > \text{factor} * \text{Long-Term Utilization}$ <p>This inequality is used to recognize increases in the Utilization value. Assuming the default factor of 1.5, the Current Utilization value must be less than or equal to 150% of the Long-Term Utilization value to be in the normal range.</p> <p>The default value for <i>factor</i> is <b>1.5</b>.</p> <p>For more information, see the description of the <b>mwtm statreps utilratio</b> command in <a href="#">mwtm statreps utilratio</a>, page B-128.</p> |

| Column       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ServRatio    | <p>In-Service values that are outside a normal range are indicated with a red status ball icon in the In-Service cell. An In-Service value is outside the normal range if the following condition is met:</p> $\text{Current In-Service} < \text{factor} * \text{Long-Term In-Service}$ <p>This inequality is used to recognize drops in the In-Service value. Assuming the default factor of 0.95, the Current In-Service value must be greater than or equal to 95% of the Long-Term In-Service value to be in the normal range.</p> <p>For more information, see the description of the <b>mwtm statreps servratio</b> command in <a href="#">mwtm statreps servratio</a>, page B-126.</p> |
| Hourly Age   | <p>Indicates the maximum number of days the MWTM should archive hourly network statistics reports. For more information, see the description of the <b>mwtm statreps hourlyage</b> and <b>mwtm rephourlyage</b> commands in <a href="#">mwtm statreps servratio</a>, page B-126.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |
| Daily Age    | <p>Indicates the maximum number of days the MWTM should archive daily network statistics reports. For more information, see the description of the <b>mwtm statreps dailyage</b> and <b>mwtm repdailyage</b> commands in <a href="#">mwtm statreps dailyage</a>, page B-119.</p>                                                                                                                                                                                                                                                                                                                                                                                                              |
| Custom Age   | <p>Indicates the maximum number of days the MWTM should archive custom network statistics reports. For more information, see the description of the <b>mwtm statreps custage</b> and <b>mwtm repcustage</b> commands in <a href="#">mwtm statreps custage</a>, page B-118.</p>                                                                                                                                                                                                                                                                                                                                                                                                                |
| Max CSV Rows | <p>Indicates the maximum number of rows the MWTM should include in export CSV files. For more information, see the description of the <b>mwtm statreps maxcsvrows</b> command in <a href="#">mwtm statreps maxcsvrows</a>, page B-123.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Web Names    | <p>Indicates whether the MWTM should show real node names or display names in web pages. For more information, see the description of the <b>mwtm webnames [display   real]</b> command in the <a href="#">mwtm webnames</a>, page B-83.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Web Util     | <p>Indicates whether the MWTM should display send and receive utilization for linksets and links as percentages or in Erlangs (E), in web pages. For more information, see the description of the <b>mwtm webutil [percent   erlangs]</b> command in <a href="#">mwtm who</a>, page B-84.</p>                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timer files  | <p>Indicates timer activities during the last report run by the MWTM. The timer file is useful for identifying how much time the MWTM spends gathering report data and generating reports.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Locating Stored ITP Reports

The MWTM stores all reports in the report files directory on the */reports* directory. If you installed the MWTM in:

- The default directory, */opt*, then the default report files directory is */opt/CSCOs/gm/reports*.
- A different directory or used the **mwtm repdir** command to specify a new directory in which the MWTM should store report files, then the default report files directory resides in that directory.

**Note**

For details on changing the default reports directory by using the **mwtm repdir** command, see [Changing the MWTM Reports Directory, page 12-65](#).

The */reports* directory contains these subdirectories:

| Subdirectory         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>/custom</i>       | <p>Contains all custom report files. These are the report files that you generate using these commands:<br/> <b>mwtm accstats</b>, <b>mwtm gttstats</b>, <b>mwtm linkstats</b>, <b>mwtm mlrstats</b>, <b>mwtm mtpevents</b>, <b>mwtm q752stats</b>, and <b>mwtm xuastats</b></p> <p><b>Note</b> A unique ID tag, specified when you enter the command, identifies each file. If the user does not specify an ID tag, the MWTM uses the process ID of the command.</p> |
| <i>/daily</i>        | <p>Contains all daily report files for these statistics:</p> <ul style="list-style-type: none"> <li>Accounting</li> <li>GTT</li> <li>MLR</li> </ul> <p>Files are stored in <i>.Z</i> format.</p>                                                                                                                                                                                                                                                                      |
| <i>/etc</i>          | <p>Contains additional files that the MWTM reporting scripts and web pages use, including the <i>nodes.include</i>, <i>linksets.include</i>, <i>nodes.exclude</i>, <i>linksets.exclude</i> and <i>filter.include</i> files, if they exist.</p>                                                                                                                                                                                                                        |
| <i>/exportdaily</i>  | <p>Contains all daily report files for these statistics:</p> <ul style="list-style-type: none"> <li>Link</li> <li>Linkset</li> <li>MLR</li> <li>Accounting</li> <li>GTT</li> <li>MSU</li> </ul> <p>Files are edited and formatted for export and stored as <i>.zip</i> files in comma-separated value (CSV) format.</p>                                                                                                                                               |
| <i>/exporthourly</i> | <p>Contains all hourly report files for these statistics:</p> <ul style="list-style-type: none"> <li>Application server</li> <li>Application server process</li> <li>Link</li> <li>Linkset</li> <li>Q.752</li> </ul> <p>Files are edited and formatted for export and stored as <i>.zip</i> files in CSV format.</p>                                                                                                                                                  |

| Subdirectory   | Description                                                                                                                                                                                                                                                                                                                                                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /exportrolling | <p>Contains all rolling report files for these statistics:</p> <ul style="list-style-type: none"> <li>• Application server</li> <li>• Application server process</li> <li>• Link</li> <li>• Linkset</li> </ul> <p>Files are edited and formatted for export and stored as .zip files in CSV format. The MWTM rebuilds the files in this subdirectory every hour.</p> |
| /hourly        | <p>Contains all hourly report files for these statistics:</p> <ul style="list-style-type: none"> <li>• Application server</li> <li>• Application server process</li> <li>• Link</li> <li>• Linkset</li> <li>• Q.752</li> </ul> <p>Files are stored in .Z format.</p>                                                                                                 |

## Changing the MWTM Reports Directory

On the server, you can change the directory in which the MWTM stores reports.

To change the MWTM report files directory, log in as the root user, as described in [Starting the MWTM Client, page 4-2](#); or, as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#), and enter:

```
cd /opt/CSC0sgm/bin
./mwtm repdir directory
```

where *directory* is the new directory.



### Note

This command copies all files in the current directory to the new directory. If you log in as the superuser and you do not own the new directory, you might not be able to copy the files. In that case, you must specify a directory that you own or log in as the root user.

## Customizing ITP Report Preferences

This table lists server CLI commands that allow you to customize your report preferences:

| Command                                            |
|----------------------------------------------------|
| <a href="#">mwtm evreps clean, page B-95</a>       |
| <a href="#">mwtm evreps cleancustom, page B-95</a> |
| <a href="#">mwtm evreps diskcheck, page B-95</a>   |
| <a href="#">mwtm evreps hourlyage, page B-96</a>   |

**Command**[mwtm evreps status, page B-97](#)[mwtm evreps timer, page B-97](#)[mwtm replog, page B-113](#)[mwtm statreps clean, page B-117](#)[mwtm statreps cleancustom, page B-118](#)[mwtm statreps custage, page B-118](#) or [mwtm repcustage, page B-112](#)[mwtm statreps dailyage, page B-119](#) or [mwtm repdailyage, page B-52](#)[mwtm statreps diskcheck, page B-119](#)[mwtm statreps servratio, page B-126](#) or [mwtm rephourlyage, page B-53](#)[mwtm statreps iplinks, page B-122](#)[mwtm statreps nullcaps, page B-125](#)[mwtm statreps servratio, page B-126](#)[mwtm statreps status, page B-126](#)[mwtm statreps timemode, page B-127](#)[mwtm statreps timer, page B-127](#)[mwtm statreps utilratio, page B-128](#)[mwtm webnames, page B-83](#)[mwtm who, page B-84](#)



# CHAPTER 13

## Editing an ITP Route Table File

---

Cisco IP Transfer Points (ITPs) use a route table to select the appropriate signaling path for each message, or signal unit, that it must forward. The route table provides the destination point code of the packet and the linkset name that it uses to forward the packet.



**Note**

---

ITP route tables do not support Virtual linksets, and the Cisco Mobile Wireless Transport Manager (MWTM) does not display Virtual linksets in the Route Table dialog box.

---

This chapter contains this information:

- [Editing an MWTM ITP Route Table File, page 13-1](#)
- [Editing a Non-MWTM ITP Route Table, page 13-16](#)

## Editing an MWTM ITP Route Table File

You use the MWTM to edit ITP route table files for an ITP.

To edit a route table file by using the MWTM, open the route table file by using one of these procedures:

- [Opening a Route Table File from a File, page 13-2](#)
- [Opening a Route Table File from a Node, page 13-3](#)
- [Opening a Route Table File from an Archive, page 13-4](#)
- [Editing ITP Route Tables, page 13-5](#)
- [Loading an Existing Route Table File, page 13-12](#)
- [Deploying a Route Table File, page 13-13](#)
- [Saving a Route Table File, page 13-13](#)
- [Reverting to the Last Saved Route Table File, page 13-15](#)

## Opening a Route Table File from a File

To open a route table file from a file, choose **Tools > Route Table Editor > From File** from the MWTM main menu, select the name of a route table file, then click **OK**.



**Note** When you open a route table from a file or archive, the MWTM preserves the order of entries that have the same Destination Point Code, Mask, and Cost.

If the chosen route table file contains incorrect linkset entries (for example, if your network configuration changed since the last time the route table file was saved), the Replace Linkset dialog box appears.

You can use the Replace Linkset dialog box to quickly replace incorrect linkset entries in route table files when your network configuration changes.

| Field or Button                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linksets That Are No Longer Valid          | Indicates the incorrect linksets in the route table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Auto Replace with Linkset                  | Replaces the highlighted incorrect linkset with a correct linkset, chosen from the drop-down list box, in all affected entries in the route table file.<br><br>To replace an incorrect linkset with a correct linkset, select an incorrect linkset in the Linksets That Are No Longer Valid table, then select a correct linkset from the Auto Replace with Linkset drop-down list box, then click <b>Apply</b> . The MWTM automatically replaces the incorrect linkset with the chosen correct linkset in all affected entries in the route table file. |
| Remove Entries Containing Selected Linkset | Removes all entries that contain the highlighted incorrect linkset from the route table file.<br><br>To remove all entries that contain an incorrect linkset from the route table file, select an incorrect linkset in the Linksets That Are No Longer Valid table, then check the Remove Entries Containing Selected Linkset check box, then click <b>Apply</b> . The MWTM automatically removes all entries that contain the incorrect linkset from the route table file.                                                                              |
| Apply                                      | Applies any changes you made to the route table file and closes the Replace Linkset dialog box. When you have corrected all incorrect linkset entries in the route table file, the <b>Apply</b> button becomes the <b>Done</b> button.                                                                                                                                                                                                                                                                                                                   |
| Done                                       | Closes the Replace Linkset dialog box and opens the Route Table dialog box.<br><br>When you have corrected all incorrect linksets in the route table file, click <b>Done</b> . The Route Table dialog box appears (Figure 13-2).                                                                                                                                                                                                                                                                                                                         |
| Cancel                                     | Closes the Replace Linkset dialog box without saving any changes to the route table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Help                                       | Shows online help for the current window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



If the chosen route table file does not contain any incorrect linkset entries, the MWTM skips the Replace Linkset dialog box and the Route Table dialog box appears ([Figure 13-2](#)).

**Related Topic:**

[Editing ITP Route Tables, page 13-5.](#)

## Opening a Route Table File from a Node

To open a route table file from a node, use one of these procedures:

- Select a network object in a window, then choose **Tools > Route Table Editor > From Node** from the MWTM main menu. (If you select an Unmanaged node, this option is dimmed and cannot be chosen.)
- Right-click a signaling point in a window, then choose **Edit > Route Table** from the right-click menu. (If you select an Unmanaged signaling point, this option is dimmed and cannot be chosen.)



**Note**

When you open a route table from a node, the MWTM cannot preserve the order of entries that have the same Destination Point Code, Mask, and Cost. Instead, the MWTM loads the entries based on the Destination Linkset. If you need to preserve the order of entries that have the same Destination Point Code, Mask, and Cost, right-click one of the entries and select **Move Up** or **Move Down** to move the entry up or down in the route table. The MWTM preserves the new order of the entries when you save the route table.

If more than one signaling point is associated with the node, the Choose Signaling Point dialog box appears, which you use to select the signaling point whose route table you want to edit.

| Field or Button      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Signaling Point List | Drop-down list box of signaling points. Select the signaling point with the point code, variant, and network name that matches the route table file you want to edit. If you select a signaling point that has the: <ul style="list-style-type: none"> <li>• Wrong variant, the MWTM shows the message:<br/>Point code out of range.</li> <li>• Correct variant but the wrong instance, the Replace Linkset dialog box appears, prompting you to replace or remove most or all of the linksets.</li> </ul> |
| OK                   | Opens the route table associated with the chosen signaling point.<br>The MWTM reads the active route table from the node and shows it in the Route Table dialog box.                                                                                                                                                                                                                                                                                                                                       |
| Cancel               | Closes the Choose Signaling Point dialog box without selecting a signaling point.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Help                 | Shows online help for the Choose Signaling Point dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Related Topic:**

[Editing ITP Route Tables, page 13-5.](#)

## Opening a Route Table File from an Archive

To open a route table file from an archive, use one of these procedures:

- Select a network object in a window, then choose **Tools > Route Table Editor > From Archive** from the MWTM main menu. (If you select an **Unmanaged** node, this option is dimmed and cannot be chosen.)
- From the Route Table dialog box, choose **File > Load from Archive**.
- From the Archive Management window, select a route table file from the list, then choose **File > Open File**.

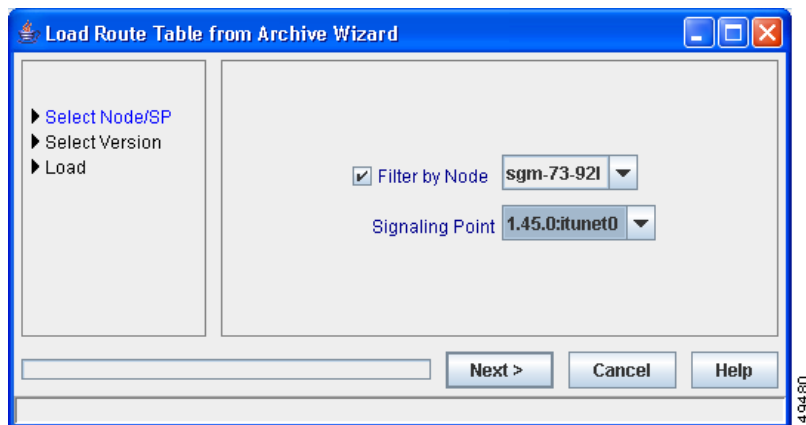


### Note

When you open a route table from a file or archive, the MWTM preserves the order of entries that have the same Destination Point Code, Mask, and Cost.

The Load Route Table from Archive wizard appears. If more than one signaling point is associated with the node, the Select Node/SP dialog box appears, which you use to select the node and signaling point whose route table you want to edit.

**Figure 13-1** Load Route Table from Archive Wizard



The left pane of the Load Route Table from Archive wizard contains:

| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Node/SP  | <p>You can select the signaling point from which the route table file should be loaded. You can optionally check the <b>Filter by Node</b> check box, which limits signaling point selection to a specific node.</p> <p>Select a signaling point and node (optional) from the drop-down list boxes in the right pane, then click <b>Next</b>. The MWTM retrieves route table filenames from the chosen signaling point.</p> <p>If no route table filenames are available, the process ends with errors. If route table filenames are available, the MWTM proceeds directly to the <b>Select Version</b> step.</p> |
| Select Version  | <p>You can select the version you want to load. Click a version to highlight it, then select <b>Next</b>. The table includes:</p> <ul style="list-style-type: none"> <li>• <b>Rev</b>—Revision number.</li> <li>• <b>Date</b>—Date and time the version was created.</li> <li>• <b>Comments</b>—Provided at the time of creation, if applicable.</li> <li>• <b>Author</b>—Initiator of the comments.</li> </ul>                                                                                                                                                                                                   |
| Load            | Loads the chosen file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Next>           | Advances to the next step in the Deployment wizard.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Cancel          | Closes the wizard without loading a file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Help            | Shows online help for the Load Route Table from Archive wizard.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Related Topic:**

[Editing ITP Route Tables, page 13-5.](#)

## Editing ITP Route Tables

You use the MWTM to edit ITP route tables for an ITP. ITP uses route tables to locate a destination linkset for a packet whose destination point code does not match the ITP's local point code.

The Route Table dialog box appears when you open a route table from one of these objects:

- **File**—See [Opening a Route Table File from a File, page 13-2](#)
- **ITP**—See [Opening a Route Table File from a Node, page 13-3](#)
- **Archive**—See [Opening a Route Table File from an Archive, page 13-4](#)

The Route Table dialog box appears.

**Figure 13-2**      *Route Table Dialog*

The Route Table dialog box contains:

- [Route Table Dialog Menu, page 13-7](#)
- [Route Table Dialog Right-Click Menu, page 13-8](#)
- [Route Table, page 13-8](#)

**Related Topic:**

[Editing an MWTM ITP Route Table File, page 13-1](#)

## Route Table Dialog Menu

The menu on the Route Table dialog box contains:

| Menu Command                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > Load from Archive (Ctrl-H)         | Opens the Load Route Table from Archive wizard, which you use to load an archived route table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| File > Load from File (Ctrl-L)            | Opens the Load File dialog, which you use to load an already existing route table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| File > Load from Signaling Point (Ctrl-F) | Opens the Choose Signaling Point dialog box ( <a href="#">Figure 13-2</a> ), which you use to select the signaling point whose route table you want to edit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| File > Revert (Ctrl-R)                    | Reverts to the last saved version of the route table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| File > Save to File (Ctrl-S)              | <p>Saves changes you made to the route table. If you are editing a route table from:</p> <ul style="list-style-type: none"> <li>An ITP (that is, if you chose <b>Tools &gt; Route Table Editor &gt; From ITP</b> from the MWTM main menu), the default filename is the name of the signaling point.</li> <li>A file (that is, if you chose <b>Tools &gt; Route Table Editor &gt; From File</b> from the MWTM main menu), the default filename is the name of the file that you are currently editing.</li> </ul> <p>The MWTM stores the modified route table file in the route table directory on the MWTM server. If you installed the MWTM in:</p> <ul style="list-style-type: none"> <li>The default directory, <i>/opt</i>, then the MWTM route table directory is <i>/opt/CSCOsgm/routes</i>.</li> <li>A different directory, then the MWTM route table directory resides in that directory.</li> </ul> |
| File > Save As                            | Opens the Save File dialog: Route Table file list, which you use to save the route table file with a new name, or overwrite an existing route table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| File > Print (Ctrl-P)                     | <p>Opens the Print window where you can:</p> <ul style="list-style-type: none"> <li>Specify options for printing.</li> <li>Print the current window.</li> <li>Save the current window to a file.</li> </ul> <p>The MWTM printing options require that you define a printer on your system. If you click <b>Print</b> and the Print window does not appear, ensure that you defined a printer on your system.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File > Find (Ctrl-F)                      | Opens the Find dialog box, which you use to find a specific character string in the window (see <a href="#">Finding Information in a Window, page 5-23</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| File > Deploy (Ctrl-Y)                    | Opens the Deployment wizard, which you use to validate a route table file, upload it to an ITP, and activate it on the ITP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Menu Command                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > Close<br>(Ctrl-W)    | Closes the Route Table dialog box. If you made any changes, the MWTM asks if you want to apply the changes before leaving the window. Click: <ul style="list-style-type: none"> <li>• <b>Yes</b> to apply the changes and close the prompt window and the Route Table dialog box.</li> <li>• <b>No</b> to close the prompt window and the Route Table dialog box without applying or saving any changes.</li> <li>• <b>Cancel</b> to close the prompt window without applying any changes. The Route Table dialog box remains open.</li> </ul> |
| Help > Topics<br>(F1)       | Shows the table of contents for the MWTM online help.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Help > Window<br>(Shift-F1) | Shows online help for the current window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Help > About<br>(F3)        | Shows build date, version, SSL support, and copyright information about the MWTM application.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Route Table Dialog Right-Click Menu

The right-click menu on the Route Table dialog box contains:

| Menu Command | Description                                                                                                                    |
|--------------|--------------------------------------------------------------------------------------------------------------------------------|
| Move Up      | Moves the chosen entry up in the route table. The MWTM preserves the new order of the entries when you save the route table.   |
| Move Down    | Moves the chosen entry down in the route table. The MWTM preserves the new order of the entries when you save the route table. |



### Note

The only entries that you can move up or down in the route table are adjacent entries that have the same **Destination Point Code**, **Mask**, and **Cost**.

## Route Table

The route table lists destination point codes and associated destination linkset names, as well as other important information used to route packets on a node.

Press **Enter** to move down to the next row in the route table; press **Tab** to move to the next field.

You can resize each column in the route table, but you cannot sort the table based on the information in one of the columns (see [Navigating Table Columns, page 5-24](#)).

| Column or Button       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title Bar              | <p>When you first open a route table, the title bar of the Route Table dialog box shows:</p> <p>MWTM: Route Table Dialog -- SP: &lt;point code:optional network name&gt;</p> <p>If you save the route table, the title bar shows:</p> <p>MWTM: Route Table Dialog -- SP: &lt;point code:optional network name&gt; -- File: &lt;filename&gt;</p> <p>If MWTM user access is enabled, and you do not have permission to edit the route table, the title bar shows:</p> <p>MWTM: Route Table Dialog (view only mode) -- SP: &lt;point code:optional network name&gt;</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Row Num                | <p>Unique number identifying each entry in the route table. You cannot edit this field, but the number might change as you add entries to or delete entries from the route table.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Destination Point Code | <p>Destination point code for packets on the chosen node. The destination point code is the point code to which a given packet is routed. To edit the destination point code, enter the new code in this field.</p> <p>If you enter a new destination point code that is less restrictive than the mask, the MWTM shows a message to that effect at the bottom of the Route Table dialog box, and performs one of these actions. If you:</p> <ul style="list-style-type: none"> <li>Modified an existing point code, the MWTM restores the previous point code.</li> <li>Entered an entirely new point code, the MWTM leaves this field blank.</li> </ul> <p>For example, a destination point code of <b>7.7.7</b>, which specifies 14 bits, is less restrictive than a mask of <b>7.255.0</b>, which specifies only 11 bits. The MWTM ignores the extra bits in the last digit of the destination point code and converts it to <b>7.7.0</b>.</p> <p>To add a new route to the route table, select the Destination Point Code field in a blank row, then fill in the field with the destination point code for the new route. When you move the cursor to another field in the row, the MWTM automatically populates the rest of the fields with the default values for those fields.</p> <p><b>Note</b> You can prevent the MWTM from automatically populating the fields with default values (see <a href="#">mwtm routetabledefs</a>, page B-115).</p> <p>You can specify the point code mask when you enter a destination point code. To do so, enter the destination point code, then a slash (/), then the number of bits in the mask. For example, if you specify <b>7.255.6/14</b>, the MWTM shows <b>7.255.7</b> in the Destination Point Code field and <b>7.255.7</b> (or <b>14</b>) in the Mask field.</p> |

| Column or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mask             | <p>Mask specifying the significant bits of the point code.</p> <p>The MWTM can display point code masks in dotted-decimal format (the default setting) or as a number of bits (see <a href="#">General Display Settings, page 5-4</a>). For:</p> <ul style="list-style-type: none"> <li>ANSI and China standard networks using the default 24-bit point code format, the default mask is <b>255.255.255</b> (or <b>24</b>).</li> </ul> <p>If the Destination Point Code is a network route with the format <b>x.x.0</b>, the default mask is <b>255.255.0</b> (or <b>16</b>).</p> <p>If the Destination Point Code is a cluster route with the format <b>x.0.0</b>, the default mask is <b>255.0.0</b> (or <b>8</b>).</p> <ul style="list-style-type: none"> <li>ITU networks using the default 14-bit point code format, the default mask is <b>7.255.7</b> (or <b>14</b>).</li> </ul> <p>If the Destination Point Code is a network route with the format <b>x.x.0</b>, the default mask is <b>7.255.0</b> (or <b>11</b>).</p> <p>If the Destination Point Code is a cluster route with the format <b>x.0.0</b>, the default mask is <b>7.0.0</b> (or <b>3</b>).</p> <ul style="list-style-type: none"> <li>NTT and TTC networks using the default 16-bit point code format, the default mask is <b>31.15.127</b> (or <b>16</b>).</li> </ul> <p>If the Destination Point Code is a network route with the format <b>x.x.0</b>, the default mask is <b>31.15.0</b> (or <b>9</b>).</p> <p>If the Destination Point Code is a cluster route with the format <b>x.0.0</b>, the default mask is <b>31.0.0</b> (or <b>5</b>).</p> <p>To edit the mask, make the changes in this field.</p> |



| Column or Button    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mask<br>(continued) | <p>If you enter a new mask, the binary conversion of the mask cannot contain ones (1) to the right of zeros (0). For example:</p> <ul style="list-style-type: none"> <li>• <b>7.255.7</b> is a valid mask because it converts to binary <b>111.11111111.111</b>.</li> <li>• <b>7.255.1</b> is <i>not</i> a valid mask because it converts to binary <b>111.11111111.001</b>.</li> </ul> <p>If you enter an invalid mask, such as <b>7.255.1</b>, a message appears to that effect at the bottom of the Route Table dialog box, and performs one of these actions. If you:</p> <ul style="list-style-type: none"> <li>• Modified an existing mask, the MWTM restores the previous mask.</li> <li>• Entered an entirely new mask, the MWTM leaves this field blank.</li> </ul> <p>If you enter a new mask that is more restrictive than the destination point code, the MWTM asks if you want to adjust the point code automatically based on the new mask. Click:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b> if you want to adjust the point code. For example, if the point code is <b>7.7.7</b>, and you enter the new mask <b>7.255.0</b>, the MWTM automatically adjusts the point code to <b>7.7.0</b>.</li> <li>• <b>No</b> if you do not want to adjust the point code. If you: <ul style="list-style-type: none"> <li>– Modified an existing mask, the MWTM restores the previous mask.</li> <li>– Entered an entirely new mask, the MWTM leaves this field blank.</li> </ul> </li> </ul> <p>If the MWTM is displaying point code masks in dotted-decimal format and you enter a number of bits, the MWTM automatically converts the number of bits to dotted-decimal format. For example, if you enter <b>24</b>, the MWTM automatically converts the mask to <b>255.255.255</b>.</p> <p>If the MWTM is displaying point code masks in bits format and you enter a mask in dotted-decimal format, the MWTM automatically converts the mask to a number of bits. For example, if you enter <b>255.255.255</b>, the MWTM automatically converts the mask to <b>24</b>.</p> |
| Cost                | <p>Cost of the route to the destination, relative to other routes. Select a cost from the drop-down list box. The valid costs range from <b>1</b> (lowest cost and highest priority) through <b>9</b> (highest cost and lowest priority).</p> <p><b>Note</b> If you configure two routes to the same node and do not specify a cost for one of them, then the cost for that node defaults automatically to <b>5</b>. The default cost appears here in the Cost column, and in the output of the <b>show cs7 route</b> command.</p> <p>Similarly, if you add a new line to this table and leave the Cost column blank, the MWTM automatically enters a default cost of <b>5</b>.</p> <p>Linksets with the same cost form a combined linkset. Do not specify more than two linksets with the same cost, under the same destination point code and mask.</p> <p>If the Destination Point Code is an adjacent point code, the default Cost is <b>1</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Destination Linkset | <p>Destination linkset associated with the destination point code. The destination linkset is also called the output linkset. To edit the destination linkset, select a destination linkset from the drop-down list box. <b>None</b> is the default setting.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Column or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| QoS              | <p>Quality of service (QoS) class of the route, that the network administrator configured. To edit the QoS class of the route, select a QoS class from the drop-down list box. Valid QoS classes range from <b>1</b> through <b>7</b>. Select <b>ALL</b> if you want the route to accept all QoS classes. <b>ALL</b> is the default value.</p> <p>When you change the QoS class for a route, the MWTM automatically changes the QoS classes for all other routes in that route set (that is, all other routes with the same Destination Point Code) to the new class.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Sort Table       | Sorts the entries in the route table field-by-field, beginning with Dest. Point Code, then Mask, Cost, Dest.Linkset, and finally QoS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Add Entry        | Scrolls to a blank row in the route table and selects the Destination Point Code field. Fill in the field with the destination point code for the new route, then fill in the rest of the fields in the row.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Delete Entry     | <p>Deletes one or more chosen rows from the table. The Confirm Deletion dialog box appears. To:</p> <ul style="list-style-type: none"> <li>• Delete the chosen rows, click <b>Yes</b>. The rows are deleted from the table and the Confirm Deletion dialog box closes.</li> <li>• Retain the chosen rows, click <b>No</b>. The rows are kept in the table and the Confirm Deletion dialog box closes.</li> <li>• Prevent MWTM from displaying the Confirm Deletion dialog box, check the <b>Do not show this again</b> check box.</li> </ul> <p><b>Note</b> If you check the <b>Do not show this again</b> check box, and you later decide you want MWTM to begin displaying the Confirm Deletion dialog box again, you must check the <b>Confirm Deletions</b> check box in the General GUI settings in the Preferences window. For more information, see the description of the <b>Confirm Deletions</b> check box in <a href="#">Startup/Exit Settings, page 5-4</a>.</p> <p>If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.</p> |

## Loading an Existing Route Table File

You use the MWTM to load a specific route table file and change the list of route table files. To load an existing route table file, use one of these procedures. Choose:

- **File > Load from Archive** from the route table menu. The Load Route Table from Archive wizard appears ([Figure 13-1](#)). For details, see [Opening a Route Table File from an Archive, page 13-4](#).
- **File > Load from Signaling Point** from the route table menu. The Choose Signaling Point dialog box appears. For details, see [Opening a Route Table File from a Node, page 13-3](#). In the Signaling Point List drop-down list box, select the signaling point with the point code, variant, and network name that matches the route table file that you want to edit, then click **OK**. The MWTM reads the active route table from the ITP and shows it in the Route Table dialog box ([Figure 13-2](#)). For details, see [Editing ITP Route Tables, page 13-5](#).
- **File > Load from File** from the route table menu. The Load File dialog: Route Table file list appears.

| Field, Button, or Icon                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                                               | Icon indicating whether the item in the table is a file or a folder.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Name                                               | Name of the route table file or folder.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Last Modified                                      | Date and time the route table file or folder was last modified.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Size (bytes)                                       | Size of the route table file or folder, in bytes.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Number of Files<br>(visible in bottom left corner) | Total number of route table files and folders.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| OK                                                 | Loads the chosen route table file, saves any changes you made to the list of files, and closes the dialog box.<br><br>To load a route table file, double-click it in the list, select it in the list and click <b>OK</b> ; or, enter the name of the file and click <b>OK</b> . The MWTM loads the route table file, saves any changes you made to the list of files, closes the Load File dialog: Route Table file list, and returns to the Route Table dialog box. |
| Delete                                             | Deletes the chosen file from the route table file list. The MWTM issues an informational message containing the name and location of the deleted file.                                                                                                                                                                                                                                                                                                               |
| Cancel                                             | Closes the dialog box without loading a route table file or saving any changes to the route table file list.                                                                                                                                                                                                                                                                                                                                                         |
| Help                                               | Shows online help for the dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Deploying a Route Table File

You use the Deployment wizard to validate a route table file, upload it to an ITP, archive the file, and activate it on the ITP. To launch the Deployment wizard for a route table file, choose **File > Deploy** from the route table menu (see [Deploying ITP Files, page 5-36](#)).

## Saving a Route Table File

You use the MWTM to save a specific route table file and change the list of route table files.

Use one of these procedures. To save the changes you made to the route table file:

- Without changing the name of the file, choose **File > Save** from the route table menu.
- With a new name, choose **File > Save As** from the route table menu. The Save File dialog: Route Table file list dialog box appears.

The MWTM stores the modified route table file in the route table file directory on the MWTM server. If you installed the MWTM in:

- The default directory, */opt*, then the MWTM route table file directory is */opt/CSCOSgm/routes*.
- A different directory, then the MWTM route table file directory resides in that directory.

You can use the **mwtm routedir** command to change the directory in which the MWTM stores ITP route table files (and to enable the TFTP path to deploy a route table; see [mwtm routedir, page B-114](#)).

**Note**

If another user modifies and saves the route table file before you save your changes, the MWTM asks if you want to overwrite that user's changes. If you do, the other user's changes are overwritten and lost. If you do not, your changes are lost, unless you save the route table file to a different filename.

| Field, Button, or Icon                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                                               | Icon indicating whether the item in the table is a file or a folder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Name                                               | Name of the route table file or folder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Last Modified                                      | Date and time the route table file or folder was last modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Size (bytes)                                       | Size of the route table file or folder, in bytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Filename                                           | Name by which you want to save the route table file.<br><br>If you create a new route table filename, you can use any letters, numbers, or characters in the name that your operating system allows. However, if you include any spaces in the new name, the MWTM converts those spaces to dashes. For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Number of Files<br>(visible in bottom left corner) | Total number of route table files and folders.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| OK                                                 | Saves any changes you made to the route table file being edited and any changes you made to the list of files and closes the dialog box.<br><br>To save the route table file with a new name, use one of these procedures. To save the file with: <ul style="list-style-type: none"> <li>• A completely new name, enter the new name and click <b>OK</b>.</li> <li>• An existing name, overwriting an old route table file, select the name in the list and click <b>OK</b>.</li> </ul> The MWTM saves the route table file with the new name, saves any changes you made to the list of files, closes the Save File dialog: Route Table file list dialog box, and returns to the Route Table dialog box.<br><br>If two or more entries in the route table have the same Destination Point Code, Mask, and Cost, the MWTM preserves the order of the entries when you save the route table. |
| Delete                                             | Deletes the chosen file from the route table file list. The MWTM issues an informational message containing the name and location of the deleted file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Cancel                                             | Closes the dialog box without saving the route table file or saving any changes to the route table file list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Help                                               | Shows online help for the dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Reverting to the Last Saved Route Table File

To revert to the last saved version of the route table file, choose **File > Revert** from the route table menu. The MWTM shows the last saved version of the file.

# Editing a Non-MWTM ITP Route Table

You use the MWTM to create and edit ITP route table files for an ITP (see [Editing an MWTM ITP Route Table File, page 13-1](#)).

If you want to edit a route table file that was created with a product other than the MWTM, to ensure that the MWTM can use the file, you must:

- 
- Step 1** Ensure that the route table file uses the MWTM route table file extension, *.rou*.
- Step 2** Place the route table file in the MWTM route table directory on the MWTM server. If you installed the MWTM in:
- The default directory, */opt*, then the MWTM route table directory is */opt/CSCOsgm/routes*.
  - A different directory, then the MWTM route table directory resides in that directory.
- Step 3** Ensure that the MWTM header lines in the file precede the ITP route table entries. The MWTM header lines use this format:

```
!! Created by MWTM 6.1.0
!! on Feb 13, 2004 6:42:54 PM
!! Do not edit this file by hand.
!v6.1.0
!ted220dbc4a
!p800:ITU:National:[net0]
```

where:

- Comment lines begin with double exclamation points (!!).
- The version line begins with **!v**. This line indicates the version of MWTM that was used to create the file.
- The timestamp line begins with **!t**. This line indicates the date and time, in hexadecimal, that the file was created.
- The point code line begins with **!p**. This line indicates the point code that the ITP used, in hexadecimal, followed by the point code variant (ANSI, China, ITU, NTT, or TTC), the network indicator (National, NationalSpare, International, or InternationalSpare), and the network name. In this example:

**!p8b0:ITU:National:[net0]**

the point code is **1.22.0**, the point code variant is **ITU**, the network indicator is **National**, and the network name is **net0**.

---



## CHAPTER 14

# Editing an ITP Global Title Translation Table

You can use the Global Title Translation (GTT) Editor of the Cisco Mobile Wireless Transport Manager (MWTM) to configure GTT entries.

A global title is an application address, such as a toll-free telephone number, calling card number, or mobile subscriber identification number. GTT is the process by which the Signaling Connection Control Part (SCCP) translates a global title into the point code and subsystem number (SSN) of the destination service switching point (SSP), where higher-layer protocol processing occurs. GTT entries reside in GTT files, which are comma-separated value (CSV) text files with point codes written in hexadecimal notation.



### Note

The MWTM 6.1 supports only GTT files with file format versions 3.1, 4.0, 4.1, 4.2, 4.3, or 4.4. You can load GTT files that use lower or higher file-format versions; but, fields or features that are unique to the lower or higher version are not visible and they disappear from the GTT file the next time you save the file. The file is saved as a version 3.1 file if the file is lower than version 3.1; or, as a version 4.4 file if the file is higher than version 4.4.

For more detailed information about GTT, including configuration procedures and scenarios, see the IP Transfer Point (ITP) feature module for Cisco IOS software release 12.2(25)SW4 or later.

This chapter contains:

- [Launching the GTT Editor, page 14-2](#)
- [Editing a GTT Table, page 14-16](#)
- [Adding a Selector to a Selector Table, page 14-17](#)
- [Adding a GTA Entry to a GTT, page 14-18](#)
- [Searching the GTA Table for GTA Digits, page 14-21](#)
- [Adding an Application Group Entry to an App Group Table, page 14-23](#)
- [Adding a MAP Entry to a GTT, page 14-24](#)
- [Adding a CPC List to a GTT, page 14-26](#)
- [Adding a GTT Address Conversion Table, page 14-26](#)
- [Adding an Entry to a GTT Conversion Table Entry, page 14-28](#)
- [Deleting Rows from a Table, page 14-29](#)
- [Creating a New GTT File, page 14-30](#)
- [Loading an Existing GTT File, page 14-31](#)

- [Loading a GTT File from a Node, page 14-33](#)
- [Loading a GTT File from the Archive, page 14-34](#)
- [Displaying the Progress Dialog Box, page 14-35](#)
- [Checking the Semantics of a GTT File, page 14-36](#)
- [Deploying a GTT File, page 14-37](#)
- [Displaying Basic Information About a GTT File, page 14-38](#)
- [Supporting Cross-Instance GTT Files, page 14-39](#)
- [Saving a GTT File, page 14-42](#)
- [Reverting to the Last Saved GTT File, page 14-44](#)

## Launching the GTT Editor

The MWTM provides you with a GTT Editor to edit GTT files. The GTT Editor runs as a separate application in the MWTM; so, it requires a separate login, just like the MWTM client.

To launch the GTT Editor, use one of these procedures:

- Choose **Tools > Global Title Translator Editor** from the MWTM main menu.
- Enter the **mwtm gttclient** command (see [mwtm gttclient, page B-98](#)).

The Startup Options dialog box appears, which you use to load a specific GTT file or create a new GTT file.

The Startup Options dialog box provides options to load GTT data from:

| Field or Button | Description                                                                                                                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New File        | Opens the Create New Table dialog box, which you use to create a new GTT file (see <a href="#">Creating a New GTT File, page 14-30</a> ). Create the new GTT file.                                                    |
| File            | Opens the Load File dialog box: GTT File List, which you use to load a specific GTT file and change the list of GTT files (see <a href="#">Loading an Existing GTT File, page 14-31</a> ). Select a GTT file to load. |
| ITP             | Opens the Load GTT from ITP wizard, which you use to choose the node and signaling point whose GTT file you want to edit (see <a href="#">Loading a GTT File from a Node, page 14-33</a> ).                           |
| Archive         | Opens the Load GTT from Archive wizard, which you use to choose the node and signaling point whose GTT file you want to edit (see <a href="#">Loading a GTT File from the Archive, page 14-34</a> ).                  |

When you close the Startup Options dialog box by creating a new GTT file or loading an existing GTT file, the GTT Editor window appears with the Selectors and GTA tab clicked.



**Figure 14-1 GTT Editor—Selectors and GTA Tab**

**Selector Table 2 Entries**

| Name      | Translation Type | Pre-Address Conversion | Post-Address Conversion | QoS |
|-----------|------------------|------------------------|-------------------------|-----|
| 2691c-2   | 34               |                        |                         | All |
| 2691ci0-1 | 22               |                        |                         | All |

**GTA Table Selector: 2691c-2 4 Entries**

| Name    | Global Title Address... | Point Co... | Routing Indic... | Subsystem Nu... | New Translation... | Application G... | Application Server ... | QoS |
|---------|-------------------------|-------------|------------------|-----------------|--------------------|------------------|------------------------|-----|
| 2691c-2 | 9                       |             | none             |                 |                    | APPGRP0-1        |                        | All |
| 2691c-2 | 8                       |             | none             |                 |                    | APPGRP0-1        |                        | All |
| 2691c-2 | 7                       |             | none             |                 |                    | APPGRP0-1        |                        | All |
| 2691c-2 | 555                     |             | none             |                 |                    | AppOneTest       |                        | All |

**App Group Table APPGRP0-1 3 Entries**

| Name      | Multiplicity | Weight Fa... | Point Code | Routing Indica... | Subsystem Number | Application Server Name | Network Name |
|-----------|--------------|--------------|------------|-------------------|------------------|-------------------------|--------------|
| APPGRP0-1 | sha          | 3            | 1.7.0      | gt                |                  |                         |              |
| APPGRP0-1 | sha          | 4            | 1.8.0      | gt                |                  |                         |              |
| APPGRP0-1 | sha          | 5            | 1.9.0      | gt                |                  |                         |              |

**MAP Table Point Code: 1.7.0 0 Entries**

| Primary Pt... | Primary S... | Multiplicity | Backup Pt... | Backup S... | Re-route if Cong... | Adja... | CPC List Name | Point Code |
|---------------|--------------|--------------|--------------|-------------|---------------------|---------|---------------|------------|
|---------------|--------------|--------------|--------------|-------------|---------------------|---------|---------------|------------|

**CPC List 0 Entries**

dhcp-64-102-82-133-cisco-com 210638

*Might need to recapture this screen with 6.1 data.*

The GTT Editor window provides a set of tabs. Each tab contains a series of tables with GTT data. Some of the tables may be blank at first, while others contain rows of data.

In each table, you can edit the values in each row by typing over the current value or selecting a new value from a drop-down list box.

To reset a cell to its previous value, press **Esc**. (If you have edited more than one cell in a row, pressing **Esc** resets all cells in the row.) To save your changes, click outside the row. Once you save your changes, pressing **Esc** does not reset the cells in the row.

To add a row to a table, select the table, then choose **Edit > Add** from the GTT menu or **Add** from the right-click menu.

To delete one or more rows from a table, select the rows, then choose **Edit > Delete** from the GTT menu or **Delete** from the right-click menu (see [Deleting Rows from a Table](#), page 14-29).

The GTT Editor window contains:

- [GTT Menu](#), page 14-4
- [GTT Editor: Selectors and GTA Tab](#), page 14-6
- [GTT Editor: App Group Tab](#), page 14-10
- [GTT Editor: MAPs Tab](#), page 14-11
- [GTT Editor: CPC Tab](#), page 14-12
- [GTT Editor: Address Conversion Tab](#), page 14-13

## GTT Menu

The menu on the GTT Editor window contains:

| Menu Command                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > New Table<br>(Ctrl-N)             | Opens the Create New Table dialog box.                                                                                                                                                                                                                                                                                                                                                                                                      |
| File > Load > Load From Archive (Ctrl-H) | <p>Opens the Load GTT from Archive wizard from which you choose the node and signaling point whose GTT file you want to edit (see <a href="#">Loading a GTT File from the Archive, page 14-34</a>).</p> <p>If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.</p>                                                                           |
| File > Load > Load From File (Ctrl-L)    | <p>Loads an already existing GTT file. The MWTM prompts you for the name of the GTT file you want to load:</p> <ul style="list-style-type: none"> <li>• Enter the name of the GTT file; or, choose the file from the list, then click <b>OK</b> to load the GTT file.</li> <li>• Click <b>Cancel</b> to close the prompt window without loading a GTT file.</li> </ul> <p>See <a href="#">Loading an Existing GTT File, page 14-31</a>.</p> |
| File > Load > Load From ITP (Ctrl-T)     | <p>Opens the Load GTT from ITP wizard, which you use to choose the node and signaling point whose GTT file you want to edit (see <a href="#">Loading a GTT File from a Node, page 14-33</a>).</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.</p>                                                                                        |
| File > Revert (Ctrl-R)                   | Reverts to the last saved version of the GTT file.                                                                                                                                                                                                                                                                                                                                                                                          |
| File > Save (Ctrl-S)                     | Saves the changes you made to the GTT file.                                                                                                                                                                                                                                                                                                                                                                                                 |
| File > Save As                           | Opens the Save File dialog box: GTT File List, which you use to save the GTT file with a new name or overwrite an existing GTT file.                                                                                                                                                                                                                                                                                                        |
| File > Semantic Check (Ctrl-K)           | Opens the Semantic Check GTT dialog box, which you use to check the semantics of a GTT file against a specific ITP.                                                                                                                                                                                                                                                                                                                         |
| File > Deploy (Ctrl-Y)                   | Opens the Deployment wizard, which you use to validate a GTT file, upload it to an ITP, and activate it on the ITP.                                                                                                                                                                                                                                                                                                                         |

| Menu Command                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > Exit<br>(Ctrl-Q)                 | <p>Closes the GTT Editor window. If you make any changes to the GTT file, the MWTM asks if you want to save the changes before leaving the window. Click:</p> <ul style="list-style-type: none"> <li><b>Yes</b> to save the changes.<br/>The MWTM opens the Save File dialog box: GTT File List, which you use to save the GTT file with a new name, or overwrite an existing GTT file.</li> <li><b>No</b> to close the prompt window.<br/>The MWTM closes the GTT Editor window without saving any changes to the GTT file.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Edit > Version and Instance<br>(Ctrl-I) | Opens the Edit GTT Table dialog box, which you use to change the variant, version, and instance number of a GTT file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Edit > Add<br>(Ctrl-E)                  | <p>Opens the Add dialog box for the chosen table.</p> <p>For example, if you click the Selector Table, opens the Selector Add dialog box.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Edit > Delete<br>(Ctrl-Delete)          | <p>Deletes one or more chosen rows from a GTT table. The Confirm Delete dialog box appears, in which you confirm the deletion. To:</p> <ul style="list-style-type: none"> <li>Delete the chosen rows, click <b>Yes</b>. The rows disappear from the table and the Confirm Delete dialog box closes.</li> <li>Retain the chosen rows, click <b>No</b>. The rows remain in the table and the Confirm Delete dialog box closes.</li> </ul> <p>You can select more than one row to delete; but, all chosen rows must reside in the same table. For example, you cannot simultaneously delete rows from the Selector Table and the MAP (mated application) Table.</p> <p>If deleting a row from a table causes one or more rows in the table to remain at the top of the page or the bottom of the next, such that no remaining entries reference the single rows, the MWTM shows the number of single rows and asks whether you also want to delete the single rows. (The MWTM shows the number of rows and not the rows themselves; because, a document could contain thousands of single rows.)</p> |
| Edit > Node Archive Management          | <p>Opens the Archive Management dialog box, which you use to manage archived GTT, route table, and MLR address table files.</p> <p>If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Edit > Node File Management             | <p>Opens the Node File Management dialog box, which you use to manage GTT files and route table files.</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Menu Command                               | Description                                                                                                                                           |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| View > Phone Number Config (Ctrl-P)        | Opens the Phone Number Lookup dialog box in which you search the GTA Table for the Global Title Address Digits for a specific selector.               |
| View > GTT Table Info (Ctrl-G)             | Opens the GTT Table Info dialog box, which shows basic information about the currently visible GTT file.                                              |
| View > Network Name Configuration (Ctrl-F) | Opens the Network Name Configuration dialog box, which maps network names to variants and network indicators, in support of cross-instance GTT files. |
| Help > Topics (F1)                         | Shows the table of contents for the MWTM online help.                                                                                                 |
| Help > Window (Shift-F1)                   | Shows online help for the current window.                                                                                                             |
| Help > About (F3)                          | Shows build date, version, SSL support, and copyright information about the MWTM application.                                                         |

## GTT Editor: Selectors and GTA Tab

Click the **Selectors and GTA** tab to display data for a specific GTT selector and see the GTA entries for that selector.

A GTT selector defines the parameters that select the translation table that the MWTM uses to translate an SCCP message to its next or final destination.

A Global Title Address (GTA) entry is associated with a selector and defines the result of a translation for a particular address mask. The result of a GTA entry can be a final translation or an intermediate translation.

The GTT Editor: Selectors and GTA tab contains:

- [Selector Table, page 14-7](#)
- [GTA Table, page 14-8](#)
- [App Group Table, page 14-8](#)
- [MAP Table, page 14-9](#)
- [CPC List, page 14-10](#)

When you click the GTT Editor: Selectors and GTA tab, the MWTM might populate the Selector Table and the other tables with data. To populate the:

- Selector Table, right-click in the table and choose **Add**. See [Adding a Selector to a Selector Table, page 14-17](#).
- GTA Table, select a row in the Selector Table. The MWTM populates the GTA Table with all associated GTA entries.

If the GTA Table remains blank, the chosen row has no associated GTA entries. You can also add entries to the GTA Table, by right-clicking in the table and choosing **Add** from the right-click menu (see [Adding a GTA Entry to a GTT, page 14-18](#)).

- App Group Table, select a row in the GTA Table that has an associated Application Group. The MWTM populates the App Group Table with all application group entries for that application group name.

You can also add entries to the App Group Table, by right-clicking in the table and choosing **Add** from the right-click menu (see [Adding an Application Group Entry to an App Group Table](#), page 14-23).

- MAP Table, select a row in the GTA Table that does not have an associated Application Group. The MWTM populates the MAP Table with all MAP entries that match the chosen row's point code-SSN combination.

To add entries to the MAP Table, right-click in the table and choose **Add** from the right-click menu (see [Adding a MAP Entry to a GTT](#), page 14-24).

- CPC List, select a row in the MAP Table that has an associated CPC List Name. The MWTM populates the CPC List with all point codes in that CPC list.

To add entries to the CPC List, right-click in the list and choose **Add** from the right-click menu (see [Adding a CPC List to a GTT](#), page 14-26).

## Selector Table

The Selector Table contains:

| Column                      | Description                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                        | Name of the selector.                                                                                                                                                                                                                                                                                                                                 |
| Translation Type            | Translation type that the selector uses. Valid values are in the range 0 through 255.                                                                                                                                                                                                                                                                 |
| Global Title Indicator      | (China, ITU, NTT, and TTC only) Global title indicator for the selector. Valid values are in the range 2 and 4.                                                                                                                                                                                                                                       |
| Numbering Plan              | (China, ITU, NTT, and TTC only) Numbering plan for the selector. Valid values are in the range 0 through 15.                                                                                                                                                                                                                                          |
| Nature of Address Indicator | (China, ITU, NTT, and TTC only) Nature of address indicator for the selector. Valid values are in the range 0 through 127.                                                                                                                                                                                                                            |
| Pre-Address Conversion      | GTT address conversion table to apply prior to performing local GTT translation. If: <ul style="list-style-type: none"> <li>• This field contains an address conversion table name, the referenced table must exist and contain at least one address-conversion entry.</li> <li>• This field is blank, no address conversion is necessary.</li> </ul> |
| Post-Address Conversion     | GTT address conversion table to apply after performing local GTT translation. If: <ul style="list-style-type: none"> <li>• This field contains an address conversion table name, the referenced table must exist and contain at least one address conversion entry.</li> <li>• This field is blank, no address conversion is necessary.</li> </ul>    |
| QoS                         | Quality of service (QoS) class of the selector. Valid QoS classes range from 1 through 7. <b>ALL</b> indicates that the selector accepts all QoS classes.                                                                                                                                                                                             |

## GTA Table

The GTA Table contains:

| Column                      | Description                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                        | Selector name for this GTA.                                                                                                                                                                                                                                                                                                                                              |
| Global Title Address Digits | Address digits for the GTA.                                                                                                                                                                                                                                                                                                                                              |
| Point Code                  | Destination point code for the GTA.                                                                                                                                                                                                                                                                                                                                      |
| Routing Indicator           | Routing indicator for the GTA. Valid values are: <ul style="list-style-type: none"> <li>• <b>none</b>—No routing indicator.</li> <li>• <b>gt</b>—Route on the global title.</li> <li>• <b>pcssn</b>—Route on the point code and SSN.</li> </ul> This field is dimmed if you check Configure By App Group (see <a href="#">Adding a GTA Entry to a GTT, page 14-18</a> ). |
| Subsystem Number            | Destination SSN for the GTA. Valid values are in the range 2 through 255.                                                                                                                                                                                                                                                                                                |
| New Translation Type        | Translation type that the GTA uses. Valid values are in the range 0 through 255.                                                                                                                                                                                                                                                                                         |
| Application Group           | Name of the application group that should provide the point code, routing indicator, and SSN that the GTA uses.                                                                                                                                                                                                                                                          |
| Application Server Name     | Name of the application server that should provide the point code, routing indicator, and SSN that the GTA uses.                                                                                                                                                                                                                                                         |
| QoS                         | Quality of service (QoS) class of the GTA. Valid QoS classes range from 1 through 7. ALL indicates that the GTA accepts all QoS classes.                                                                                                                                                                                                                                 |

## App Group Table

The App Group Table contains:

| Column       | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name         | Name of the application group.<br><br>For ITPs with multiple instances enabled, do not use the same application group name in two or more different instances. For example, if you use application group name <i>appgrp1</i> in instance 1, then do not use <i>appgrp1</i> in instance 0, or any other instance.                                                                                                 |
| Multiplicity | Multiplicity setting for the application group. Valid values are: <ul style="list-style-type: none"> <li>• <b>cgp</b>—Use SCCP calling party address (CGPA) load sharing, if available. CGPA load sharing uses a weighting factor to choose the destination.</li> <li>• <b>cos</b>—Use the destination with the least cost, if available.</li> <li>• <b>sha</b>—Share equally among all destinations.</li> </ul> |

| Column                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Weight Factor or Cost   | <p>If you set multiplicity to <b>cgp</b>, this field specifies the relative weighting factor of the application group. Choose a relative cost, <b>1</b> through <b>999</b>, from the drop-down list box. The default value is <b>1</b>.</p> <p>If you set multiplicity to <b>cos</b> or <b>sha</b>, this field specifies the relative cost of the application group. Choose a relative cost, <b>1</b> through <b>8</b>, from the drop-down list box. The default value is <b>1</b>.</p> <p>For file format 4.4, the cost range is from <b>1</b> through <b>64</b>.</p> |
| Point Code              | Destination point code for the application group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Routing Indicator       | <p>Routing indicator for the application group. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>none</b>—No routing indicator.</li> <li>• <b>gt</b>—Route on the global title. This is the default routing indicator.</li> <li>• <b>pcssn</b>—Route on the point code and SSN.</li> </ul>                                                                                                                                                                                                                                                            |
| Subsystem Number        | Destination SSN for the application group. Valid values are in the range 2 through 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Application Server Name | Name of the application server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Network Name            | Network name that the application group uses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Translation Type        | (Appears only for file format version 4.4) Translation type that the selector uses. Valid values are in the range 0 through 255.                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## MAP Table

The MAP Table contains:

| Column                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Pt. Code      | Primary point code for the MAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Primary SSN           | Primary SSN for the MAP. Valid values are in the range 2 through 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Multiplicity          | <p>Multiplicity setting for the MAP. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>dom</b>—Dominant. Always translate to the primary point-code-SSN combination if it is available. Translate to the backup point code-SSN combination only if the primary combination is not available.</li> <li>• <b>sha</b>—Share equally between the primary point-code-SSN combination and the backup point-code-SSN combination.</li> <li>• <b>sol</b>—Solitary MAP. No alternate if the point code or SSN is not available.</li> </ul> |
| Backup Pt. Code       | Backup point code for the MAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Backup SSN            | Backup SSN for the MAP. Valid values are in the range 2 through 255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Re-route if Congested | <p>Indicates whether to route the MAP to the backup point-code-SSN combination if the primary combination is congested. If you:</p> <ul style="list-style-type: none"> <li>• Check the check box, you route the MAP to the backup combination when the primary combination is congested.</li> <li>• Uncheck the check box, you do not route the MAP to the backup.</li> </ul>                                                                                                                                                                     |

| Column        | Description                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adjacency     | Indicates whether to consider a point-code-SSN combination adjacent to the local node for SCCP management. If you: <ul style="list-style-type: none"> <li>• Check the check box, you do consider the point code-SSN combination adjacent to the local node.</li> <li>• Uncheck the check box, you do not consider the point code-SSN combination adjacent to the local node.</li> </ul> |
| CPC List Name | Name of the CPC list associated with this MAP.                                                                                                                                                                                                                                                                                                                                          |

## CPC List

The CPC List contains:

| Field      | Description                         |
|------------|-------------------------------------|
| Point Code | Point codes in the chosen CPC list. |

## GTT Editor: App Group Tab

Click the **App Group** tab to display data for application groups. The App Group tab shows the same information as the Selectors and GTA tab; but, from the perspective of the application groups.

An application group is an alternative result for the explicit point code and SSN in a GTA entry. You can use an application group entry for:

- Intermediate translation.
- Load-sharing across more than two destinations.
- Load-sharing of intermediate translation.

The GTT Editor: App Group tab contains:

- [App Group Table, page 14-8](#)
- [MAP Table, page 14-9](#)
- [CPC List, page 14-10](#)
- [Selector Table, page 14-7](#)
- [GTA Table, page 14-8](#)

When you click the **GTT Editor: App Group** tab, the App Group Table and Selector Table might contain data. To:

- Add entries to the App Group Table, right-click in the table and choose **Add** from the right-click menu (see [Adding an Application Group Entry to an App Group Table, page 14-23](#)).
- Add entries to the Selector Table, right-click in the table and choose **Add** from the right-click menu (see [Adding a Selector to a Selector Table, page 14-17](#)).
- Populate the MAP Table, select a row in the App Group Table. The MAP Table contains all MAP entries that match the chosen row's point code-SSN combination.

You can also add entries to the MAP Table, by right-clicking in the table and choosing **Add** from the right-click menu (see [Adding a MAP Entry to a GTT, page 14-24](#)).



- Populate the CPC List, select a row in the MAP Table that has an associated CPC List Name. The CPC List contains all point codes in that CPC list.

You can also add entries to the CPC List, by right-clicking in the list and choosing **Add** from the right-click menu (see [Editing an ITP Global Title Translation Table, page 14-1](#)).

- Populate the GTA Table, select a row in the Selector Table. The GTA Table contains all associated GTA entries.

If the GTA Table remains blank, the chosen row has no associated GTA entries. You can also add entries to the GTA Table, by right-clicking in the table and choosing **Add** from the right-click menu (see [Editing an ITP Global Title Translation Table, page 14-1](#)).

You can also add entries to the Selector Table, by right-clicking in the list and choosing **Add** from the right-click menu (see [Adding a Selector to a Selector Table, page 14-17](#)).

## GTT Editor: MAPs Tab

Click the **MAPs** tab if you are primarily interested in displaying data for MAPs. The MAPs tab shows the same information as the Selectors and GTA tab, but from the perspective of the MAPs.

A mated application (MAP) entry has two uses:

- The SCCP application uses MAP entries internally to track point code states and SSN states, such as congestion and availability.
- To define backups or alternates for point code-SSN combination.

The GTT Editor: Maps tab contains:

- [MAP Table, page 14-9](#)
- [CPC List, page 14-10](#)
- [Selector Table, page 14-7](#)
- [GTA Table, page 14-8](#)
- [App Group Table, page 14-8](#)

When you launch the GTT Editor: MAPs tab, the MAP Table and Selector Table might or might not be populated with data. To:

- Add entries to the MAP Table, right-click in the table and choose **Add** from the right-click menu (see [Adding a MAP Entry to a GTT, page 14-24](#)).
- Add entries to the Selector Table, right-click in the table and choose **Add** from the right-click menu (see [Adding a Selector to a Selector Table, page 14-17](#)).

- Populate the CPC List, select a row in the MAP Table that has an associated CPC List Name. The CPC List contains all point codes in that CPC list.

You can also add entries to the CPC List, by right-clicking in the list and choosing **Add** from the right-click menu (see [Editing an ITP Global Title Translation Table, page 14-1](#)).

- Populate the App Group Table and GTA Table, select a row in the MAP Table. The App Group Table and GTA Table contain all application group and GTA entries that match the chosen row's point code-SSN combination.

If the App Group Table or GTA Table remains blank, the chosen row has no associated application group or GTA entries.

You can add entries to the App Group Table, by right-clicking in the table and choosing **Add** from the right-click menu (see [Adding an Application Group Entry to an App Group Table, page 14-23](#)).

You can add entries to the GTA Table, by right-clicking in the table and choosing **Add** from the right-click menu (see [Editing an ITP Global Title Translation Table, page 14-1](#)).

## GTT Editor: CPC Tab

A concerned point code (CPC) is a node that should be notified when the status of the associated SSN changes.

Click the **CPC** tab if you are primarily interested in displaying data for concerned point code names. The CPC tab appears.

The GTT Editor: CPC tab contains:

- [Concerned Pt. Code Name List, page 14-13](#)
- [CPC List, page 14-10](#)
- [MAP Table, page 14-9](#)

When you launch the GTT Editor: CPC tab, the Concerned Pt. Code Name List contains data. To populate the CPC List and MAP Table, select a row in the Concerned Pt. Code Name List. The CPC List and MAP Table contain all point codes and MAP entries that match that concerned point code name.

## Concerned Pt. Code Name List

The Concerned Pt. Code Name List contains:

| Field         | Description                                                                            |
|---------------|----------------------------------------------------------------------------------------|
| CPC List Name | Name of the CPC list to add. Enter an alphanumeric string between 1 and 12 characters. |
| CPC List      | List of point codes associated with the entered CPC list name.                         |

To copy one or more point codes from one CPC list to another, select a CPC list in the CPC List Name column. The MWTM shows the point codes that are associated with that CPC list in the Point Code column. Select one or more of the point codes and drag them to the new CPC list.

**Note**

The MWTM copies the point codes to the new CPC list; it does not move them from the old CPC list. If you want to move the point codes, you must copy them to the new CPC list, then delete them from the old CPC list.

## GTT Editor: Address Conversion Tab

You use GTT address conversion tables to specify mappings such as E.212-to-E.214 address conversion and E.212-to-E.164 address conversion in ITU networks.

Click the **Address Conversion** tab to display GTT address conversion tables. The Address Conversion tab appears.

The GTT Editor: Address Conversion tab contains:

- [Address Conversion Table, page 14-14](#)
- [Conversion Entry Table, page 14-14](#)
- [Selector Table for Address Conversion, page 14-15](#)

## Address Conversion Table

The Address Conversion Table contains:

| Field                       | Description                                                                                                                                                                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                        | Name of the GTT address conversion table. Enter a 1- to 12-character name.                                                                                                                                                                               |
| Numbering Plan              | (China, ITU, NTT, and TTC only) Numbering plan associated with the address conversion table. For all addresses that are converted, the numbering plan is converted to the value of this field.<br>The valid range is 0 to 15.                            |
| Nature of Address Indicator | (China, ITU, NTT, and TTC only) Nature of address indicator associated with the address conversion table. For all addresses that are converted, the nature of address indicator is converted to the value of this field.<br>The valid range is 0 to 127. |

## Conversion Entry Table

The Conversion Entry Table contains:

| Field                       | Description                                                                                                                                                                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In Address                  | Input SCCP address entry. Enter an address as a 1- to 15-digit hexadecimal string.                                                                                                                                                                                                                         |
| Out Address                 | Output SCCP address entry. Enter an address as a 1- to 15-digit hexadecimal string.                                                                                                                                                                                                                        |
| Numbering Plan              | (China, ITU, NTT, and TTC only) Numbering plan associated with this entry in the address conversion table. If specified, the value of this field overrides the value of the Numbering Plan field in the Address Conversion Table for this entry.<br>The valid range is 0 to 15.                            |
| Nature of Address Indicator | (China, ITU, NTT, and TTC only) Nature of address indicator associated with this entry in the address conversion table. If specified, the value of this field overrides the value of the Nature of Address Indicator field in the Address Conversion Table for this entry.<br>The valid range is 0 to 127. |

| Field           | Description                                                                                                                                                                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encoding Scheme | The encoding scheme to be used for output GTT address: <ul style="list-style-type: none"> <li>Unknown—Encoding scheme is not specified at the address level</li> <li>bcdOdd—Use BCD odd encoding scheme</li> <li>bcdEven—Use BCD even encoding scheme</li> <li>National—National specific</li> </ul> |
| Remove Digits   | Specifies the number of digits that should be removed from the original address prefix when the in-address prefix is matched                                                                                                                                                                         |

## Selector Table for Address Conversion

The Selector Table for Address Conversion contains:

| Column                      | Description                                                                                                                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                        | Name of the selector.                                                                                                                                                                                                                                                                                          |
| Translation Type            | Translation type that the selector uses. Valid values are in the range 0 through 255.                                                                                                                                                                                                                          |
| Global Title Indicator      | Global title indicator for the selector. Valid values are in the range 2 and 4.                                                                                                                                                                                                                                |
| Numbering Plan              | (China, ITU, NTT, and TTC only) Numbering plan for the selector. Valid values are in the range 0 through 15.                                                                                                                                                                                                   |
| Nature of Address Indicator | (China, ITU, NTT, and TTC only) Nature of address indicator for the selector. Valid values are in the range 0 through 127.                                                                                                                                                                                     |
| Pre-Address Conversion      | GTT address conversion table to apply prior to performing local GTT translation.<br><br>If this field contains an address conversion table name, the referenced table must exist and it must contain at least one address-conversion entry.<br><br>If this field is blank, no address conversion is necessary. |
| Post-Address Conversion     | GTT address conversion table to apply after performing local GTT translation.<br><br>If this field contains an address-conversion table name, the referenced table must exist and it must contain at least one address conversion entry.<br><br>If this field is blank, no address conversion is necessary.    |
| QoS                         | Quality of service (QoS) class of the selector. Valid QoS classes range from 1 through 7. ALL indicates that the selector accepts all QoS classes.                                                                                                                                                             |

# Editing a GTT Table

You use the MWTM to change the variant and instance number associated with a GTT file.

To change the variant and instance number associated with a GTT file choose **Edit > Version and Instance** from the GTT menu. The Edit GTT Table dialog box appears.

| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Variant         | SS7 protocol variant. You cannot edit this field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Version         | <p>Version of the file format that the GTT uses. Valid versions are:</p> <ul style="list-style-type: none"> <li>• <b>3.1</b>—Corresponds to ITP software releases 12.2(4)MB9 and 12.2(4)MB9a. Two or more entries in the same application group can have the same cost. This version is the default in the MWTM.</li> <li>• <b>4.0</b>—Corresponds to ITP software release 12.2(4)MB10 or higher. Supports multiple instances on a single node.</li> <li>• <b>4.1</b>—Corresponds to ITP software release 12.2(20)SW or higher. Supports multiple instances on a single node.</li> <li>• <b>4.2</b>—Corresponds to ITP software release 12.2(21)SW1 or higher. Supports subsystem numbers equal to zero (0) for GTA entries and application group entries.</li> <li>• <b>4.3</b>—Corresponds to these ITP software releases: <ul style="list-style-type: none"> <li>– 12.2(25)SW1 or higher</li> <li>– 12.2(18)IXA or higher</li> <li>– 12.4(11)SW or higher</li> </ul> Supports latest encoding scheme (not for ANSI).</li> <li>• <b>4.4</b>—Corresponds to these ITP software releases: <ul style="list-style-type: none"> <li>– 12.2(18)IXE or higher</li> <li>– 12.4(15)SW or higher</li> </ul> Supports higher destination cost and removing digits.</li> </ul> <p>The MWTM 6.1 supports only GTT files with file format versions 3.1, 4.0, 4.1, 4.2, 4.3, or 4.4. You can load GTT files that use lower or higher file format versions; but, fields or features that are unique to the lower or higher version are not visible and they disappear from the GTT file the next time you save. The MWTM automatically saves the file as a version 3.1 file if the file is lower than version 3.1; or, as a version 4.4 file if the file is higher than version 4.4.</p> |
| Instance Number | <p>Number of the instance that the GTT uses. Valid IDs are 0 to 7. The default instance number is 0.</p> <p>This list box is available only if you choose version 4.0.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Network Name    | <p>Network name that the GTT uses.</p> <p>If you change the network name for an existing GTT file, the new network name must use the same variant.</p> <p>This field is available only if you choose version 4.1 or higher.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Field or Button | Description                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK              | Saves the changes to the GTT file.<br><br>Enter or choose values for the new variant and instance number, then click <b>OK</b> . The MWTM saves your changes to the GTT file.                                |
| Cancel          | Closes the Edit GTT Table dialog box without saving any changes to the GTT file.<br><br>To close the Edit GTT Table dialog box at any time without saving any changes to the GTT file, click <b>Cancel</b> . |
| Help            | Shows online help for the current window.                                                                                                                                                                    |

## Adding a Selector to a Selector Table

You use the MWTM to add a selector to a GTT. A GTT selector defines the parameters that select the translation table used to translate an SCCP message to its next or final destination.

To add a new selector to a Selector Table, choose a Selector Table in the GTT Editor window, then use one of these procedures. From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

The Selector Add dialog box appears.

| Field or Button           | Description                                                                                                                                                                                                                                                                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Selector Name             | Name of the selector to add. Enter 1- to 12-character alphanumeric string.                                                                                                                                                                                                                                     |
| Translation Type          | Translation type that the selector uses. Enter a value in the range <b>0</b> through <b>255</b> .                                                                                                                                                                                                              |
| Global Title Indicator    | (China, ITU, NTT, and TTC only) Global title indicator for the selector. Choose a value from the drop-down list box. Valid values are: <ul style="list-style-type: none"> <li>• <b>2</b></li> <li>• <b>4</b></li> </ul> The default value is 4.                                                                |
| Numbering Plan            | (China, ITU, NTT, and TTC only) Numbering plan for the selector. Enter a value in the range <b>0</b> through <b>15</b> .<br><br>This field is dimmed if Global Title Indicator is set to 2.                                                                                                                    |
| Nature of Addr. Indicator | (China, ITU, NTT, and TTC only) Nature of address indicator for the selector. Enter a value in the range <b>0</b> through <b>127</b> .<br><br>This field is dimmed if Global Title Indicator is set to 2.                                                                                                      |
| Pre-Conversion Table Name | GTT address conversion table to apply prior to performing local GTT translation.<br><br>If this field contains an address conversion table name, the referenced table must exist and it must contain at least one address conversion entry.<br><br>If this field is blank, no address conversion is necessary. |

| Field or Button            | Description                                                                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Post-Conversion Table Name | GTT address conversion table to apply after performing local GTT translation.<br><br>If this field contains an address conversion table name, the referenced table must exist and it must contain at least one address conversion entry.<br><br>If this field is blank, no address conversion is necessary. |
| QoS                        | Quality of service (QoS) class of the selector. Choose a value from the drop-down list box. Valid QoS classes range from 1 through 7. Choose <b>ALL</b> if you want the selector to accept all QoS classes. The default value is <b>ALL</b> .                                                               |
| Add                        | Adds the selector to the GTT.<br><br>Enter or choose values for the new selector, then click <b>Add</b> . The MWTM adds the selector to the Selector Table.                                                                                                                                                 |
| Close                      | Closes the Selector Add dialog box.<br><br>When you finish adding selectors, click <b>Close</b> .                                                                                                                                                                                                           |
| Help                       | Shows online help for the current window.                                                                                                                                                                                                                                                                   |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Adding a GTA Entry to a GTT

You use the MWTM to add a Global Title Address (GTA) entry to a GTT. A GTA entry is associated with a selector and defines the result of a translation for a particular address mask. The result of a GTA entry can be a final translation or an intermediate translation.

To add a new GTA entry to a GTA Table, choose a selector in the GTT Editor window and a GTA Table; then, use one of these procedures.

From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

The GTA Add dialog box appears.

| Field                     | Description                                                                                                                                                                                                                         |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Selector Name             | Name of the selector associated with this GTA. You cannot edit this field.                                                                                                                                                          |
| Global Title Addr. Digits | Address digits for the GTA. Enter a 1- to 15-digit hexadecimal string.                                                                                                                                                              |
| QoS                       | Quality of service (QoS) class of the GTA. Choose a value from the drop-down list box. Valid QoS classes range from 1 through 7. Choose <b>ALL</b> if you want the GTA to accept all QoS classes. The default value is <b>ALL</b> . |



| Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure By Point Code              | <p>Indicates whether to configure the GTA by point code. To configure the GTA by point code, click this radio button.</p> <p>The MWTM makes the Config By Point Code fields available, and dims the Config By App Group fields. This is the default setting.</p>                                                                                                                                           |
| Configure By App Group               | <p>Indicates whether to configure the GTA by application group. To configure the GTA by application group, click this radio button.</p> <p>The MWTM makes the Config By App Group fields available and, dims the Config By Point Code fields.</p>                                                                                                                                                          |
| Configure By Application Server Name | <p>Indicates whether to configure the GTA by application server name. To configure the GTA by application server name, click this radio button.</p> <p>The MWTM replaces the Config By Point Code fields with the Config By Application Server name fields, and dims the Config By App Group fields.</p>                                                                                                   |
| Point Code                           | <p>Destination point code for the GTA. Enter a point code.</p> <p>This field is available only if you choose Configure By Point Code.</p>                                                                                                                                                                                                                                                                  |
| Routing Indicator                    | <p>Routing indicator for the GTA. Choose a value from the drop-down list box. Valid values are:</p> <ul style="list-style-type: none"> <li><b>gt</b>—Route on the global title. This is the default routing indicator.</li> <li><b>pcssn</b>—Route on the point code and SSN.</li> </ul> <p>This field is available only if you chose Configure By Point Code or Configure By Application Server Name.</p> |
| Subsystem Number                     | <p>Destination SSN for the GTA. Enter a value in the range <b>2</b> through <b>255</b>.</p> <p>This field is mutually exclusive with the New Translation Type field.</p> <p>This field is available only if you chose Configure By Point Code or Configure By Application Server Name.</p>                                                                                                                 |
| New Translation Type                 | <p>Translation type that the GTA uses. Enter a value in the range <b>0</b> through <b>255</b>.</p> <p>This field is mutually exclusive with the Subsystem Number field.</p> <p>This field is available only if you chose Configure By Point Code or Configure By Application Server Name.</p>                                                                                                              |
| App. Group                           | <p>Name of the application group that should provide the point code, routing indicator, and SSN that the GTA uses. Enter the name of an application group.</p> <p>This field is available only if Configure By App Group is checked (see <a href="#">Adding a GTA Entry to a GTT, page 14-18</a>).</p>                                                                                                     |
| Application Server Name              | <p>Name of the application server that should provide the point code, routing indicator, and SSN that the GTA uses. Enter the name of an application server.</p> <p>This field is available only if you chose Configure By Application Server Name.</p>                                                                                                                                                    |

| Field                                | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configure By Point Code              | <p>Indicates whether to configure the GTA by point code. To configure the GTA by point code, click this radio button.</p> <p>The MWTM makes the Config By Point Code fields available, and dims the Config By App Group fields. This is the default setting.</p>                                                                                                                                           |
| Configure By App Group               | <p>Indicates whether to configure the GTA by application group. To configure the GTA by application group, click this radio button.</p> <p>The MWTM makes the Config By App Group fields available and, dims the Config By Point Code fields.</p>                                                                                                                                                          |
| Configure By Application Server Name | <p>Indicates whether to configure the GTA by application server name. To configure the GTA by application server name, click this radio button.</p> <p>The MWTM replaces the Config By Point Code fields with the Config By Application Server name fields, and dims the Config By App Group fields.</p>                                                                                                   |
| Point Code                           | <p>Destination point code for the GTA. Enter a point code.</p> <p>This field is available only if you choose Configure By Point Code.</p>                                                                                                                                                                                                                                                                  |
| Routing Indicator                    | <p>Routing indicator for the GTA. Choose a value from the drop-down list box. Valid values are:</p> <ul style="list-style-type: none"> <li><b>gt</b>—Route on the global title. This is the default routing indicator.</li> <li><b>pcssn</b>—Route on the point code and SSN.</li> </ul> <p>This field is available only if you chose Configure By Point Code or Configure By Application Server Name.</p> |
| Subsystem Number                     | <p>Destination SSN for the GTA. Enter a value in the range <b>2</b> through <b>255</b>.</p> <p>This field is mutually exclusive with the New Translation Type field.</p> <p>This field is available only if you chose Configure By Point Code or Configure By Application Server Name.</p>                                                                                                                 |
| New Translation Type                 | <p>Translation type that the GTA uses. Enter a value in the range <b>0</b> through <b>255</b>.</p> <p>This field is mutually exclusive with the Subsystem Number field.</p> <p>This field is available only if you chose Configure By Point Code or Configure By Application Server Name.</p>                                                                                                              |
| App. Group                           | <p>Name of the application group that should provide the point code, routing indicator, and SSN that the GTA uses. Enter the name of an application group.</p> <p>This field is available only if Configure By App Group is checked (see <a href="#">Adding a GTA Entry to a GTT, page 14-18</a>).</p>                                                                                                     |
| Application Server Name              | <p>Name of the application server that should provide the point code, routing indicator, and SSN that the GTA uses. Enter the name of an application server.</p> <p>This field is available only if you chose Configure By Application Server Name.</p>                                                                                                                                                    |

| Field | Description                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Add   | Adds the GTA to the GTT.<br>Enter or choose values for the new GTA entry, then click <b>Add</b> . The MWTM adds the GTA entry to the GTA Table. |
| Close | Closes the GTA Add dialog box.<br>When you finish adding GTA entries, click <b>Close</b> to close the GTA Add dialog box.                       |
| Help  | Shows online help for the current window.                                                                                                       |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Searching the GTA Table for GTA Digits

You use the MWTM to search the GTA Table for the Global Title Address Digits for a specific selector. The MWTM shows the entries that contain the GTA digits in the GTA Table.

To search the GTA Table, click the **Selectors and GTA** tab in the GTT Editor window, then choose **View > Phone Number Config** from the GTT menu. The Phone Number Lookup dialog box appears.

**Figure 14-2** Phone Number Lookup Dialog Box

| Table, Field, or Button           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Selector Table                    | <p>Selector Table associated with the GTA Table to search. Choose one or more Selector Tables.</p> <p>For descriptions of the fields in this table, see <a href="#">Selector Table, page 14-7</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Phone Number                      | <p>GTA digits to search for in the GTA Table.</p> <p>Choose a Selector Table and enter a telephone number or prefix as a 1- to 15-digit hexadecimal string with no spaces, dashes, or other special characters.</p> <p>For example, to search for a specific telephone number, such as 919-555-6384, enter <b>9195556384</b>. To search for all entries that begin with the 919-555 telephone prefix, enter <b>919555</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Perform Lookup                    | <p>Launches the search for the GTA digits. If:</p> <ul style="list-style-type: none"> <li>It finds one or more matching entries, shows the entries that contain the GTA digits in the GTA Table.</li> <li>The Selector Table being searched performs pre-address conversion, the converted address, numbering plan, and nature of address indicator are visible in the <b>Pre-Address Conversion Results</b> field.</li> <li>The Selector Table being searched performs post-address conversion, the converted address, numbering plan, and nature of address indicator are visible in the Post-Address Conversion Results field.</li> <li>It does not find matching entries or the Selector Table has no associated GTA Table, an error message appears at the bottom of the window:<br/> <code>Could not find GTA for selector and phone number</code></li> </ul> |
| Pre-Address Conversion Entry Used | <p>Entry in the GTT address conversion table used for pre-address conversion, if the Selector Table being searched performs pre-address conversion.</p> <p>For China, ITU, NTT, and TTC variants, pre-address conversion might result in a numbering plan or nature of address indicator that is different from the chosen Selector Table. If this occurs, the MWTM searches for a selector in the Selector Table that matches the new numbering plan and nature of address indicator. If the MWTM:</p> <ul style="list-style-type: none"> <li>Finds a matching selector, it uses that selector to complete the search.</li> <li>Does not find a matching selector, the search fails.</li> </ul>                                                                                                                                                                    |
| Pre-Address Conversion Results    | Results of the pre-address conversion (converted address, numbering plan, and nature of address indicator), if the Selector Table being searched performs pre-address conversion.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Selector Entry Used               | <p>Selector Entry that was searched.</p> <p>For descriptions of the fields in this table, see <a href="#">Selector Table, page 14-7</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| GTA Entry Found                   | <p>GTA Table in which the GTA digits reside.</p> <p>For descriptions of the fields in this table, see <a href="#">GTA Table, page 14-8</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| MAP Table                         | <p>MAP Table, if any, associated with the GTA Table in which the GTA digits were found.</p> <p>For descriptions of the fields in this table, see <a href="#">MAP Table, page 14-9</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Table, Field, or Button            | Description                                                                                                                                                                         |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPC List                           | CPC List, if any, associated with the GTA Table in which the GTA digits reside.<br>For descriptions of the fields in this list, see <a href="#">CPC List, page 14-10</a> .          |
| Post-Address Conversion Entry Used | Entry in the GTT address conversion table used for post-address conversion, if the Selector Table being searched performs post-address conversion.                                  |
| Post-Address Conversion Results    | Results of the post-address conversion (converted address, numbering plan, and nature of address indicator), if the Selector Table being searched performs post-address conversion. |

**Related Topic:**

[Launching the GTT Editor, page 14-2.](#)

## Adding an Application Group Entry to an App Group Table

You use the MWTM to add an application group to a GTT. An application group is an alternative result for the explicit point code and SSN in a GTA entry. You can use an application group entry for:

- Intermediate translation.
- Load-sharing across more than two destinations.
- Load-sharing of intermediate translation.

To add an application group to a GTT, choose an App Group Table in the GTT Editor window, then use one of these procedures.

From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

The App Group Add dialog box appears.

| Field or Button       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| App. Group            | Name of the application group to add. Enter 1- to 12-character alphanumeric string.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Multiplicity          | Multiplicity setting for the application group. Choose a value from the drop-down list box. Valid values are: <ul style="list-style-type: none"> <li>• <b>cos</b>—Use the destination with the least cost, if available.</li> <li>• <b>sha</b>—Share equally between all destinations. This is the default value.</li> </ul>                                                                                                                                                         |
| Weight Factor or Cost | If Multiplicity is set to <b>cgp</b> , this field specifies the relative weighting factor of the application group. Choose a relative cost, <b>1</b> through <b>999</b> , from the drop-down list box. The default value is <b>1</b> .<br><br>If Multiplicity is set to <b>cos</b> or <b>sha</b> , this field specifies the relative cost of the application group. Choose a relative cost, <b>1</b> through <b>8</b> , from the drop-down list box. The default value is <b>1</b> . |

| Field or Button         | Description                                                                                                                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Point Code              | Destination point code for the application group. Click this radio button and enter a point code. This field is mutually exclusive with the Application Server Name field.                      |
| Application Server Name | Name of the application server. Click this radio button and enter an application server name. This field is mutually exclusive with the Point Code field.                                       |
| Routing Indicator       | Routing indicator for the application group. Choose a value from the drop-down list box.                                                                                                        |
| Network Name            | Network name that the application group uses. Choose a network name from the drop-down list box.                                                                                                |
| Subsystem Number        | Destination SSN for the application group. Enter a value in the range <b>2</b> through <b>255</b> .                                                                                             |
| Add                     | Adds the application group to the GTT.<br>Enter or choose values for the new application group entry, then click <b>Add</b> . The MWTM adds the application group entry to the App Group Table. |
| Close                   | Closes the App Group Add dialog box.<br>When you finish adding application group entries, click <b>Close</b> to close the App Group Add dialog box.                                             |
| Help                    | Shows online help for the current window.                                                                                                                                                       |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Adding a MAP Entry to a GTT

You use the MWTM to add a mated application (MAP) entry to a GTT.

A MAP entry has two purposes:

- The SCCP application uses them internally to track point-code states and SSN states, such as congestion and availability.
- To define backups or alternates for point-code-SSN combination.

To add a MAP entry, choose a MAP Table in the GTT Editor window, then use one of these procedures.

From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

(Optional) To add a new MAP entry to a MAP Table, choose a MAP Table, then use one of these procedures.

From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

The MAP Add dialog box appears.

| Field or Button       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Pt. Code      | Primary point code for the MAP. Enter a point code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Primary SSN           | Primary SSN for the MAP. Enter a value in the range <b>2</b> through <b>255</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Multiplicity          | <p>Multiplicity setting for the MAP. Choose a value from the drop-down list box. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>dom</b>—Dominant. Always translate to the primary point-code-SSN combination if it is available. Translate to the backup point-code-SSN combination only if the primary combination is not available.</li> <li>• <b>sha</b>—Share equally between the primary point-code-SSN combination and the backup point code-SSN combination. This is the default value.</li> <li>• <b>sol</b>—Solitary MAP. No alternate if the point code or SSN is not available.</li> </ul> |
| Backup Pt. Code       | Backup point code for the MAP. Enter a point code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Backup SSN            | Backup SSN for the MAP. Enter an a value in the range <b>2</b> through <b>255</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| CPC List Name         | Name of the CPC list to be associated with this MAP. Enter a CPC list name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Re-route if Congested | <p>Indicates whether the MAP should be routed to the backup point code-SSN combination if the primary combination is congested. If you:</p> <ul style="list-style-type: none"> <li>• Want to route the MAP to the backup combination when the primary combination is congested, check the check box.</li> <li>• Do not want to route the MAP to the backup, uncheck the check box. This is the default setting.</li> </ul>                                                                                                                                                                                               |
| Adjacency             | <p>Indicates whether a point code-SSN combination should be considered adjacent to the local node for SCCP management. If you:</p> <ul style="list-style-type: none"> <li>• Want the point code-SSN combination be considered adjacent to the local node, check the check box.</li> <li>• Do not want the point code-SSN combination be considered adjacent to the local node, uncheck the check box. This is the default setting.</li> </ul>                                                                                                                                                                            |
| Add                   | <p>Adds the MAP to the GTT.</p> <p>Enter or choose values for the new MAP entry, then click <b>Add</b>. The MWTM adds the MAP entry to the MAP Table.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Close                 | <p>Closes the MAP Add dialog box.</p> <p>When you finish adding MAP entries, click <b>Close</b> to close the MAP Add dialog box.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Help                  | Shows online help for the current window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Adding a CPC List to a GTT

You use the MWTM to add a new concerned point code (CPC) list to a GTT. A CPC is a node that should be notified when the status of the associated SSN changes.

To add a new CPC list, choose a Concerned Pt. Code Name List or a CPC List in the GTT Editor window, then use one of these procedures. From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

The CPC Add dialog box appears.

| Field or Button         | Description                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPC List Name           | Name of the CPC list to be added. Enter 1- to 12-character alphanumeric string.                                                                        |
| Concerned Pt. Code List | One or more CPCs to be added to the new CPC list. Enter one or more CPCs, separated by spaces.                                                         |
| Add                     | Adds the CPC list to the GTT.<br><br>Enter or choose values for the new CPC list, then click <b>Add</b> . The MWTM adds the CPC list to the MAP Table. |
| Close                   | Closes the CPC Add dialog box.<br><br>When you finish adding CPC lists, click <b>Close</b> to close the CPC Add dialog box.                            |
| Help                    | Shows online help for the current window.                                                                                                              |

## Adding a GTT Address Conversion Table

You use the MWTM to add a new address conversion table to a GTT. To do so, choose an Address Conversion Table in the GTT Editor window, then use one of these procedures. From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

The Address Conversion Add dialog for a Table window appears.

| Field or Button           | Description                                                                                                                                                                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                      | Name of the GTT address conversion table. Enter a 1- to 12-character name.                                                                                                                                                                                   |
| Numbering Plan            | (China, ITU, NTT, and TTC only) Numbering plan associated with the address conversion table. For all addresses that are converted, the numbering plan is converted to the value of this field.<br><br>The valid range is 0 to 15.                            |
| Nature of Addr. Indicator | (China, ITU, NTT, and TTC only) Nature of address indicator associated with the address conversion table. For all addresses that are converted, the nature of address indicator is converted to the value of this field.<br><br>The valid range is 0 to 127. |



| Field or Button | Description                                                                                                                                                                                       |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add             | Adds the address conversion table to the GTT.<br>Enter or choose values for the new Address Conversion Table, then click <b>Add</b> . The MWTM adds the Address Conversion Table to the GTT file. |
| Close           | Closes the Address Conversion Add dialog box for a table.<br>When you finish adding Address Conversion Tables, click <b>Close</b> to close the Address Conversion Add dialog box for a table.     |
| Help            | Shows online help for the current window.                                                                                                                                                         |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Adding an Entry to a GTT Conversion Table Entry

You use the MWTM to add a new entry to a GTT Conversion Entry Table. To do so, choose a Conversion Entry Table in the Address Conversion tab of the GTT Editor, then use one of these procedures. From the:

- GTT menu, choose **Edit > Add**.
- Right-click menu, choose **Add**.

The Address Conversion Add dialog for an entry window appears.

| Field or Button                 | Description                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                            | Name of the GTT address conversion table. Enter a 1- to 12-character name. If the table name does not already exist, the MWTM creates a new address conversion table with this name.                                                                                                                            |
| Table Numbering Plan            | (China, ITU, NTT, and TTC only) Numbering plan associated with the address conversion table. For all addresses that are converted, the numbering plan is converted to the value of this field.<br><br>The valid range is 0 to 15.                                                                               |
| Table Nature of Addr. Indicator | (China, ITU, NTT, and TTC only) Nature of address indicator associated with the address conversion table. For all addresses that are converted, the nature of address indicator is converted to the value of this field.<br><br>The valid range is 0 to 127.                                                    |
| In Address                      | Input SCCP address entry. Enter an address as a 1- to 15-digit hexadecimal string.                                                                                                                                                                                                                              |
| Out Address                     | Output SCCP address entry. Enter an address as a 1- to 15-digit hexadecimal string.                                                                                                                                                                                                                             |
| Numbering Plan                  | (China, ITU, NTT, and TTC only) Numbering plan associated with this entry in the address conversion table. If specified, the value of this field overrides the value of the Numbering Plan field in the Address Conversion Table, for this entry.<br><br>The valid range is 0 to 15.                            |
| Nature of Address Indicator     | (China, ITU, NTT, and TTC only) Nature of address indicator associated with this entry in the address conversion table. If specified, the value of this field overrides the value of the Nature of Address Indicator field in the Address Conversion Table, for this entry.<br><br>The valid range is 0 to 127. |
| Encoding Scheme                 | <ul style="list-style-type: none"> <li>• Unknown - encoding scheme is not specified at the address level.</li> <li>• bcdOdd - Use BCD odd encoding scheme</li> <li>• bcdEven - Use BCD even encoding scheme</li> <li>• National - national specific</li> </ul>                                                  |
| Remove Digits                   | Specifies the number of digits that should be removed from the original address prefix when the in-address prefix is matched.                                                                                                                                                                                   |

| Field or Button | Description                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add             | Adds the address conversion table to the GTT.<br>Enter or choose values for the new entry, then click <b>Add</b> . The MWTM adds the entry to the Conversion Entry Table.    |
| Close           | Closes the Address Conversion Add dialog box for a table.<br>When you finish adding entries, click <b>Close</b> to close the Address Conversion Add dialog box for an entry. |
| Help            | Shows online help for the current window.                                                                                                                                    |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Deleting Rows from a Table

To delete one or more rows from a table, select the rows, then choose **Edit > Delete** from the GTT menu or **Delete** from the right-click menu. The Confirm Delete dialog box appears to confirm the deletion. To:

- Delete the chosen rows, click **Yes**. The rows are deleted from the table and the Confirm Delete dialog box closes.
- Retain the chosen rows, click **No**. The rows are kept in the table and the Confirm Delete dialog box closes.

You can select more than one row to delete, but all chosen rows must be in the same table. For example, you cannot delete rows from both the Selector Table and the MAP Table at the same time.

If deleting a row from a table causes one or more rows in the table to remain at the top of the page or the bottom of the next, such that no remaining entries reference the single rows, the MWTM shows the number of single rows and asks whether you want to also delete the single rows. (The MWTM shows the number of rows and not the rows themselves, because there could be thousands of single rows.)

## Creating a New GTT File

You use the MWTM to create a new GTT file. To do so, choose **File > New Table** from the GTT menu. The Create New Table dialog box appears.

| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Variant         | SS7 protocol variant. Choose a variant from the drop-down list box. Valid variants are: <ul style="list-style-type: none"><li>• <b>ANSI</b></li><li>• <b>China</b></li><li>• <b>ITU</b></li><li>• <b>NTT</b></li><li>• <b>TTC</b></li></ul>                                                                                                                                                                                                                                                                                                                                                                                 |
| Version         | Version of the file format that the GTT uses. Choose a version from the drop-down list box. Valid versions are: <ul style="list-style-type: none"><li>• <b>3.1</b>—Corresponds to ITP software releases 12.2(4)MB9 and 12.2(4)MB9a. Two or more entries in the same application group can have the same cost. This is the default version in the MWTM.</li><li>• <b>4.0</b>—Corresponds to ITP software release 12.2(4)MB10 or higher. Supports multiple instances on a single node.</li><li>• <b>4.1</b>—Corresponds to ITP software release 12.2(20)SW or higher. Supports multiple instances on a single node.</li></ul> |

| Field or Button        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version<br>(continued) | <ul style="list-style-type: none"> <li>• <b>4.2</b>—Corresponds to ITP software release 12.2(21)SW1 or higher. Supports subsystem numbers equal to zero (0) for GTA entries and application group entries.</li> <li>• <b>4.3</b>—Corresponds to these ITP software releases: <ul style="list-style-type: none"> <li>– 12.2(25)SW1 or higher</li> <li>– 12.2(18)IXA or higher</li> <li>– 12.4(11)SW or higher</li> </ul> Supports latest encoding scheme (not for ANSI).</li> <li>• <b>4.4</b>—Corresponds to these ITP software releases: <ul style="list-style-type: none"> <li>– 12.2(18)IXE or higher</li> <li>– 12.4(15)SW or higher</li> </ul> Supports higher destination cost and removing digits.</li> </ul> <p>The MWTM 6.1 supports only GTT files with file format versions 3.1, 4.0, 4.1, 4.2, 4.3, or 4.4. You can load GTT files that use lower or higher file format versions; but, fields or features that are unique to the lower or higher version are not visible and they are removed from the GTT file the next time it is saved. The file is saved as a version 3.1 file if the file is lower than version 3.1, or as a version 4.4 file if the file is higher than version 4.4.</p> |
| Instance Number        | <p>Number of the instance that the GTT uses. Choose an instance number from the drop-down list box. Valid IDs are <b>0</b> to <b>7</b>. The default instance number is <b>0</b>.</p> <p>This list box is available only if you chose version 4.0.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Network Name           | <p>Network name that the GTT uses. Choose a network name from the drop-down list box. When you choose the network name, The MWTM automatically sets the corresponding variant in the Variant field.</p> <p>If you change the network name for an existing GTT file, the new network name must use the same variant.</p> <p>This list box is available only if you chose version 4.1 or higher.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| OK                     | <p>Creates the new GTT file and closes the Create New Table dialog box.</p> <p>Choose a variant, version, and instance for the new GTT file, then click <b>OK</b>. The MWTM creates the new GTT file and closes the Create New Table dialog box.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Cancel                 | Closes the Create New Table dialog box without creating a new GTT file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Help                   | Shows online help for the current window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Loading an Existing GTT File

You use the MWTM to load a specific GTT file and change the list of GTT files.

When you load a GTT file, the name of the server associated with the GTT Editor and the filename are visible in the window name:

```
MWTM: GTT Editor -- mwtm-sun8 -- GTT.File.1
```

If you have not yet loaded or saved a GTT file, the MWTM displays a No File Loaded message in place of the GTT filename.

**Note**

The MWTM 6.1 supports only GTT files with file format versions 3.1, 4.0, 4.1, 4.2, 4.3, or 4.4. You can load GTT files that use lower or higher file-format versions; but, fields or features that are unique to the lower or higher version are not visible and they disappear from the GTT file the next time you save. The file is saved as a version 3.1 file if the file is lower than version 3.1, or as a version 4.4 file if the file is higher than version 4.4.

To load an existing GTT file, or to change the list of GTT files, choose **File > Load > Load From File** from the GTT menu. The Load File dialog box: GTT File List appears.

| Field or Button                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                                               | Icon indicating whether the item in the table is a file or a folder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Name                                               | Name of the GTT file or folder.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Last Modified                                      | Date and time the GTT file or folder was last modified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Size (bytes)                                       | Size of the GTT file or folder, in bytes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Number of Files<br>(visible in bottom left corner) | Total number of GTT files and folders.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| OK                                                 | <p>Loads the chosen GTT file, saves any changes you make to the list of files, closes the Load File dialog box: GTT File List, opens the Progress dialog box, and begins loading the GTT file.</p> <p>To load a GTT file, double-click it in the list; select it in the list and click <b>OK</b>; or enter the name of the file and click <b>OK</b>. The MWTM closes the Load File dialog box: GTT File List and the Progress dialog box appears.</p> <p>The Progress dialog box shows the progress of the GTT file load, as well as any messages that appear while loading the file.</p> <p>When the file is loaded, click <b>OK</b>. The MWTM closes the Progress dialog box, loads the GTT file, and returns to the GTT Configuration window.</p> |
| Delete                                             | Deletes the chosen file from the GTT file list. The MWTM issues an informational message containing the name and location of the deleted file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Cancel                                             | Closes the dialog box without loading a GTT file or saving any changes to the GTT file list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Help                                               | Shows online help for the dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Related Topics:**

- [Launching the GTT Editor, page 14-2](#)
- [Loading a GTT File from a Node, page 14-33](#)
- [Loading a GTT File from the Archive, page 14-34](#)

## Loading a GTT File from a Node

You use the Load GTT from Node wizard to choose the node and signaling point whose GTT file you want to edit.

To launch the Load GTT from Node wizard, choose **File > Load > Load From Node** from the GTT menu. Or, from the Startup Options dialog box, choose **Load GTT Data From: Node**. If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

The Load GTT from Node wizard appears.

**Figure 14-3**      *Load GTT from Node Wizard*

The left pane of the Load GTT from Node wizard contains:

| Step           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Node/SP | <p>You can choose the signaling point from which to load the GTT file. You can optionally check the <b>Filter by Node</b> check box, which limits signaling point selection to a specific node.</p> <p>Choose a signaling point and node (optional) from the drop-down list boxes, then click <b>Next</b>. The MWTM retrieves GTT filenames from the chosen signaling point.</p> <p>If no GTT filenames are available, the process ends with errors. If GTT filenames are available, the MWTM proceeds directly to the Login step.</p> |
| Login          | <p>You can log in to the signaling point. Once you have logged in initially, the MWTM skips this step. Enter the:</p> <ul style="list-style-type: none"><li>• Log in user name and password.</li><li>• Enable user name and password.</li></ul> <p><b>Note</b> To avoid entering user name and password information each time, you can set up credentials (see <a href="#">Configuring Login Credentials, page 3-20</a>).</p>                                                                                                          |
| Load           | Reads the GTT table from the node and loads it into the GTT Editor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

The bottom line of the Load GTT from Node wizard contains:

| Field or Button   | Description                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Progress Bar      | Indicates that the file is being validated or uploaded.                                                                                         |
| Show Log/Hide Log | Shows or hides the session between the MWTM and the node.                                                                                       |
| Next >            | Advances to the next step in the wizard.                                                                                                        |
| Finish            | Closes the wizard. The <b>Finish</b> button appears when deployment completes successfully; or, when it detects errors and cancels the process. |
| Cancel            | Closes the wizard without deploying the file.                                                                                                   |
| Help              | Shows online help for the wizard.                                                                                                               |

#### Related Topics:

- [Launching the GTT Editor, page 14-2](#)
- [Loading a GTT File from the Archive, page 14-34](#)

## Loading a GTT File from the Archive

You use the Load GTT from Archive wizard to choose the node and signaling point whose archived GTT file you want to edit.

To launch the Load GTT from Archive wizard, choose **File > Load > Load From Archive** from the GTT menu; or, from the Startup Options dialog box, choose **Load GTT Data From: Archive**. If you implement MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

The Load GTT from Archive wizard appears.

**Figure 14-4** Load GTT from Archive Wizard





The left pane of the Load GTT from Archive wizard contains:

| Step           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Node/SP | <p>You can choose the signaling point from which to load the GTT file. You can optionally check the <b>Filter by Node</b> check box, which limits signaling-point selection to a specific node.</p> <p>Choose a signaling point and node (optional) from the drop-down list boxes, then click <b>Next</b>. The MWTM retrieves GTT filenames from the chosen signaling point.</p> <p>If no GTT filenames are available, the process ends with errors. If GTT filenames are available, the MWTM proceeds directly to the Select Version step.</p> |
| Select Version | Select a previously deployed version of the configuration from the archive.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Load           | Checks the archived GTT file for errors and loads the file into the GTT Editor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

The bottom line of the Load GTT from Archive wizard contains:

| Field or Button | Description                                                                                                                   |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Progress Bar    | Indicates that the file is being validated or uploaded.                                                                       |
| Next >          | Advances to the next step in the wizard.                                                                                      |
| Finish          | Closes the wizard. The Finish button appears when deployment is successful; or, it encounters errors and cancels the process. |
| Cancel          | Closes the wizard without deploying the file.                                                                                 |
| Help            | Shows online help for the wizard.                                                                                             |

## Displaying the Progress Dialog Box

The Progress dialog box shows the percent of a GTT file that was loaded, saved, or checked semantically, as well as any messages that appear while loading or checking the file.

To display the Progress dialog box, use one of these procedures.

Choose:

- **File > Load > Load From File** or **Load From ITP** from the GTT menu, then select a GTT file from the Load File dialog box: GTT File List and click **OK**.
- **File > Save As** from the GTT menu, then select a GTT file from the Load File dialog box: GTT File List and click **OK**.
- **File > Semantic Check** from the GTT menu, then enter an ITP's name or IP address in the Semantic Check GTT dialog box and click **OK**.

The Progress dialog box appears.

| Field or Button | Description                                                               |
|-----------------|---------------------------------------------------------------------------|
| Progress Bar    | Indicates the percent of the GTT file that was loaded, saved, or checked. |
| Messages        | Messages that appear while loading, saving, or checking the GTT file.     |

| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK              | Closes the Progress dialog box.<br><br>This button is dimmed until the MWTM finishes loading, saving, or checking the GTT file; or, until you click <b>Cancel</b> to stop loading, saving, or checking the file.<br><br>When the file is loaded, saved, or checked, click <b>OK</b> . The MWTM closes the Progress dialog box and returns to the GTT Configuration window. |
| Cancel          | Stops loading, saving, or checking the GTT file.<br><br>This button is dimmed when the MWTM finishes loading, saving, or checking the GTT file; or, if loading, saving, or checking stops.                                                                                                                                                                                 |
| Help            | Shows online help for the current window.                                                                                                                                                                                                                                                                                                                                  |

**Related Topics:**

- [Checking the Semantics of a GTT File, page 14-36](#)
- [Launching the GTT Editor, page 14-2](#)
- [Loading an Existing GTT File, page 14-31](#)
- [Saving a GTT File, page 14-42](#)

## Checking the Semantics of a GTT File

The MWTM strongly recommends that you check the semantics of a GTT file against a specific ITP and validate this data in the GTT file:

- **ITP Point Code**—For version 2.0 GTT files, the point code in the GTT file must differ from the primary, secondary, or capability point code of the ITP. If the file is the same, the MWTM generates an error. This restriction is not for GTT files of version 3.0 or later.
- **Route Table**—The ITP route table must contain all point codes in the GTT file, other than the primary, secondary, or capability point code of the ITP. If the route table does not contain the point codes, the MWTM generates an error.
- **Route Status**—All route entries for point codes in the GTT file, other than the ITP's primary, secondary, or capability point code, must be available. If they are not, the MWTM generates a warning.
- **GTA and Application Group**—If an application server configures the GTA or the application group, then that application server must reside on the ITP. If it does not, the MWTM generates an error.

If the application server resides on the ITP, but it is not available, the MWTM generates a warning.

For example, ITP limits XUA configuration to instance 0. The MWTM semantic check verifies that XUA is not configured on any other instance.

To check the semantics of a GTT file, choose **File > Semantic Check** from the GTT menu. The Semantic Check GTT dialog box appears.

| Field or Button        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ITP Name or IP Address | Name or IP address of the ITP against which to check the GTT file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| OK                     | <p>Closes the Semantic Check GTT dialog box and opens the Progress dialog box, which shows the progress of the semantic check for the GTT file.</p> <p>Enter the name or IP address of an ITP, and click <b>OK</b>. The MWTM closes the Semantic Check GTT dialog box and opens the Progress dialog box.</p> <p>The Progress dialog box shows the progress of the semantic check for the GTT file and any messages that appear while checking the file.</p> <p>After the check, click <b>OK</b>. The MWTM closes the Progress dialog box and returns to the Semantic Check GTT dialog box.</p> |
| Cancel                 | Closes the Semantic Check GTT dialog box without checking the semantics of the GTT file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Note**

You can also use the **mwtm checkgtt** command to semantics of a GTT file (see [mwtm checkgtt](#), page B-91).

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Deploying a GTT File

You use the Deployment wizard to validate a GTT file, upload it to an ITP, archive the file, and activate it on the ITP. To launch the Deployment wizard for a GTT file, choose **File > Deploy** from the GTT menu (see [Deploying ITP Files, page 5-36](#)).

## Displaying Basic Information About a GTT File

You use the MWTM to view basic information about the current GTT file. Choose **View > GTT Table Info** from the GTT menu. The GTT Table Info dialog box appears.

| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filename        | Name of the GTT file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Version         | <p>Version of the file format that the GTT uses. Valid versions are:</p> <ul style="list-style-type: none"> <li>• <b>3.1</b>—Corresponds to ITP software releases 12.2(4)MB9 and 12.2(4)MB9a. Two or more entries in the same application group can have the same cost. This is the default version in the MWTM.</li> <li>• <b>4.0</b>—Corresponds to ITP software release 12.2(4)MB10 or higher. Supports multiple instances on a single node.</li> <li>• <b>4.1</b>—Corresponds to ITP software release 12.2(20)SW or higher. Supports multiple instances on a single node.</li> <li>• <b>4.2</b>—Corresponds to ITP software release 12.2(21)SW1 or higher. Supports subsystem numbers equal to zero (0) for GTA entries and application group entries.</li> <li>• <b>4.3</b>—Corresponds to these ITP software releases: <ul style="list-style-type: none"> <li>– 12.2(25)SW1 or higher</li> <li>– 12.2(18)IXA or higher</li> <li>– 12.4(11)SW or higher</li> </ul> Supports latest encoding scheme (not for ANSI).</li> <li>• <b>4.4</b>—Corresponds to these ITP software releases: <ul style="list-style-type: none"> <li>– 12.2(18)IXE or higher</li> <li>– 12.4(15)SW or higher</li> </ul> Supports higher destination cost and removing digits.</li> </ul> <p>The MWTM 6.1 supports only GTT files with file format versions 3.1, 4.0, 4.1, 4.2, 4.3, or 4.4. You can load GTT files that use lower or higher file format versions; but, fields or features that are unique to the lower or higher version are not visible and they disappear from the GTT file the next time you save. The file is saved as a version 3.1 file if the file is lower than version 3.1 or as a version 4.4 file if the file is higher than version 4.4.</p> |
| Variant         | <p>SS7 protocol variant. Valid variants are:</p> <ul style="list-style-type: none"> <li>• <b>ANSI</b></li> <li>• <b>China</b></li> <li>• <b>ITU</b></li> <li>• <b>NTT</b></li> <li>• <b>TTC</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Network Name    | <p>Network name that the GTT file uses.</p> <p>This field appears only for GTT files of version 4.1 or higher.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Field or Button | Description                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Instance Number | Number of the instance that the GTT uses. Valid numbers are <b>0</b> to <b>7</b> . The default instance number is <b>0</b> .<br><br>If no instance is associated with the GTT, this field contains N/A. This field appears only for GTT files of version 4.0. |
| Last Modified   | Date and time the GTT file was last modified.                                                                                                                                                                                                                 |
| Total Entries   | Total number of entries in the GTT file.                                                                                                                                                                                                                      |
| OK              | Closes the GTT Table Info dialog box.                                                                                                                                                                                                                         |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

## Supporting Cross-Instance GTT Files

You use the ITP Multiple Instance feature to connect an ITP to more than one network at the same time, each with specific variant and network indicator values. The ITP treats each combination of variant and network indicator as a separate instance with its own local point code, routing table, and GTT file on the ITP. Instances in the same network must have the same network name.

In support of the Multiple Instance feature, ITP Instance Translation enables the conversion of packets between instances of any variants. Each instance is a separate domain with a defined variant, network indicator, ITP point code, optional capability point code, and optional secondary point code.

For more information about the ITP Multiple Instance and Instance Translation features, see the IP Transfer Point (ITP) feature module for Cisco IOS software release 12.2(4)MB10 or later.

GTT files that support the Multiple Instance and Instance Translation features are called cross-instance GTT files, because they contain application groups that reference point codes in other GTT files.

To handle cross-instance GTT files, the MWTM uses a server-wide network name mapping file, which maps the available network names to GTT variants and network indicators. The MWTM looks up network names in the file to parse point codes correctly, based on the user's cross-instance configuration.

When the MWTM discovers your network, it automatically creates and populates the network name-mapping file. Therefore, in most cases, you do not need to manually create the network name mapping file. For more information about running Discovery, see [Managing and Deploying ITP Files, page 5-25](#).

In some cases, you might want to create the network name mapping file manually; for example, if you have not run Discovery yet, but you want to prepare for a future GTT configuration. Also, while you cannot change or delete entries that the MWTM automatically populated, you can add entries manually, and you can change or delete those manual entries.

To create the network name mapping file manually; or, to add, change, or delete manual entries, choose **View > Network Name Configuration** from the GTT menu. If you have implemented MWTM User-Based Access, this option is available to users with authentication level System Administrator (level 5). The Network Name Configuration dialog box appears.

The Network Name Configuration dialog box contains:

- [Network Name Configuration Dialog Box Menu, page 14-40](#)
- [Network Name Configuration Dialog Box Table, page 14-41](#)

## Network Name Configuration Dialog Box Menu

The menu on the Network Name Configuration dialog box contains:

| Menu Command                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > Revert<br>(Ctrl-R)   | Loads the most recent network name mapping file from the MWTM server.<br><br>If the MWTM discovers new entries for the network name mapping file while you are editing a GTT file (for example, if it adds a new network instance or it discovers a new network), the GTT Editor is unaware of the new entries and they are not visible in the Network Name Configuration dialog box. To see the new entries in the dialog box, choose <b>File &gt; Revert</b> . (You can also restart the GTT Editor to automatically load the most recent network name mapping file from the MWTM server.) |
| File > Save<br>(Ctrl-S)     | Saves the changes you make to the network name mapping file.<br><br>After you add, change, or delete entries and save the file, the MWTM uses the file the next time it discovers the network. However, if the MWTM discovers entries that conflict with manual entries in the file, the MWTM uses (and shows in the Network Name Configuration dialog box) the discovered entries, not the manual entries.                                                                                                                                                                                  |
| File > Print<br>(Ctrl-P)    | Prints the contents of the network name mapping file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| File > Close<br>(Ctrl-W)    | Closes the network name mapping file without saving any additions, changes, or deletions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Edit > Add<br>(Alt-A)       | Adds an entry to the network name mapping file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Edit > Delete<br>(Delete)   | Deletes the chosen entry from the network name mapping file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Help > Topics<br>(F1)       | Shows the table of contents for the MWTM online help.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Help > Window<br>(Shift-F1) | Shows online help for the current window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Help > About<br>(F3)        | Shows build date, version, SSL support, and copyright information about the MWTM application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Network Name Configuration Dialog Box Table

The Network Name Configuration dialog box table contains:

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Name      | Network name that the GTT file uses.<br><br>If you change the network name for an existing GTT file, the new network name must use the same variant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Variant           | SS7 protocol variant. Valid variants are: <ul style="list-style-type: none"><li>• <b>ANSI</b></li><li>• <b>China</b></li><li>• <b>ITU</b></li><li>• <b>NTT</b></li><li>• <b>TTC</b></li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Network Indicator | Type of call that is placed. Valid values are: <ul style="list-style-type: none"><li>• <b>National</b>—National-bound call. The MWTM routes national calls through the national network.</li><li>• <b>NationalSpare</b>—National-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates networks.</li><li>• <b>International</b>—International-bound call. The MWTM forwards international-bound calls to an STP pair that acts as an international gateway.</li><li>• <b>InternationalSpare</b>—International-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates networks.</li></ul> |
| Discovered        | Indicates whether the MWTM (Yes) or a user manually (No) discovered the entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Related Topic:**

[Editing an ITP Global Title Translation Table, page 14-1.](#)

# Saving a GTT File

You use the MWTM to save a specific GTT file and change the list of GTT files.



## Note

The MWTM 6.1 supports only GTT files with file format versions 3.1, 4.0, 4.1, 4.2, 4.3, or 4.4. You can load GTT files that use lower or higher file format versions; but, fields or features that are unique to the lower or higher version are not visible and they disappear from the GTT file the next time you save. The file is saved as a version 3.1 file if the file is lower than version 3.1 or as a version 4.4 file if the file is higher than version 4.4.

To save the changes made to a GTT file or change the list of GTT files, use one of these procedures. To save the changes you have made to the GTT file:

- Without changing the name of the file, choose **File > Save** from the GTT menu.
- With a new name, choose **File > Save As** from the GTT menu. The Save File dialog box: GTT File List appears.

| Field or Button                                    | Description                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                                               | Icon indicating whether the item in the table is a file or a folder.                                                                                                                                                                                                                                                                                    |
| Name                                               | Name of the GTT file or folder.                                                                                                                                                                                                                                                                                                                         |
| Last Modified                                      | Date and time the GTT file or folder was last modified.                                                                                                                                                                                                                                                                                                 |
| Size (bytes)                                       | Size of the GTT file or folder, in bytes.                                                                                                                                                                                                                                                                                                               |
| Filename                                           | Name by which you want to save the GTT file.<br><br>If you create a new GTT filename, you can use any letters, numbers, or characters in the name that your operating system allows. However, if you include any spaces in the new name, the MWTM converts those spaces to hyphens (-). For example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i> . |
| Number of Files<br>(visible in bottom left corner) | Total number of GTT files and folders.                                                                                                                                                                                                                                                                                                                  |



| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK              | <p>Saves the GTT file or any changes you make to the list of files and closes the dialog box.</p> <p>To save the GTT file with a new name, use one of these procedures. To save the file with:</p> <ul style="list-style-type: none"> <li>A completely new name, enter the new name and click <b>OK</b>.</li> <li>An existing name, overwriting an old GTT file, choose the name from the list and click <b>OK</b>.</li> </ul> <p>The MWTM closes the Save File dialog box: GTT File List and the Progress dialog box appears.</p> <p>The Progress dialog box shows the progress of the GTT file save, as well as any messages that appear while saving the file.</p> <p>When the file is saved, click <b>OK</b>. The MWTM closes the Progress dialog box, saves the GTT file with the new name, and returns to the GTT Configuration window.</p> <p><b>Note</b> If another user modifies and saves the GTT file before you save your changes, the MWTM asks if you want to overwrite that user's changes. If you do, the other user's changes are overwritten and lost. If you choose not to, your changes are lost; unless you save the GTT file to a different filename.</p> |
| Delete          | Deletes the chosen file from the GTT file list. An informational message appears that contains the name and location of the deleted file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Cancel          | Closes the dialog box without saving the GTT file or any changes to the GTT file list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Help            | Shows online help for the dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

When you are ready to exit the GTT Editor window, choose **File > Exit** from the GTT menu.

If you make any changes to the GTT file, the MWTM asks if you want to save the changes before leaving the window. Click:

- Yes** to save the changes.

The MWTM opens the Save File dialog box: GTT File List, which you use to save the GTT file with a new name, or overwrite an existing GTT file.

- No** to close the prompt window.

The MWTM closes the GTT Editor window without saving any changes to the GTT file.

By default, GTT files reside in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the default directory is */opt/CSCOs/gtm/gtt*.
- A different directory, then the default directory resides in that directory.

To change the directory in which the MWTM stores GTT files, use the **mwtm gttmdir** command (see [mwtm gttmdir](#), page B-98).

## Reverting to the Last Saved GTT File

To revert to the last saved version of the GTT file, choose **File > Revert** from the GTT menu. The MWTM shows the last saved version of the file.



# CHAPTER 15

## Editing ITP MLR Address Table Files

---

You use the Cisco Mobile Wireless Transport Manager (MWTM) to configure Multi-Layer Routing (MLR) address table files by using the MWTM Address Table Editor. You can:

- Create new address table files.
- Load existing address table files.
- Edit address table files.
- Perform semantic checks on address table files.
- Deploy address table files to an ITP.
- Save address table files.

If you implement MWTM User-Based Access, the Address Table Editor is available to users with authentication level Network Operator (level 3) and higher.

For more detailed information about address tables, including configuration procedures and scenarios, see the *IP Transfer Point (ITP)* feature module for Cisco IOS software release 12.2(25)SW3 or later.

This chapter contains:

- [Launching the Address Table Editor, page 15-2](#)
- [Creating a New Address Table File, page 15-6](#)
- [Loading an Existing Address Table File, page 15-8](#)
- [Loading an Address Table File from a Node, page 15-10](#)
- [Loading an Address Table File from the Archive, page 15-12](#)
- [Working in Address Table Files, page 15-14](#)
- [Editing Address Table Properties, page 15-17](#)
- [Checking the Semantics of an Address Table File, page 15-17](#)
- [Deploying an Address Table File, page 15-18](#)
- [Displaying Basic Information About an Address Table File, page 15-19](#)
- [Listing Archived Address Tables, page 15-20](#)
- [Creating Network Name Mapping Files, page 15-20](#)
- [Saving an Address Table File, page 15-23](#)
- [Reverting to the Last Saved Address Table File, page 15-25](#)

# Launching the Address Table Editor

The Address Table Editor runs as a separate application in the MWTM, so it requires a separate log in, just like the MWTM client.

If you implement MWTM User-Based Access, the Address Table Editor is available to users with authentication level Network Operator (level 3) and higher.

To launch the Address Table Editor, use one of these procedures:

- Choose **Tools > Address Table Editor** from the MWTM main menu.
- Enter the **mwtm atblclient** command (see [mwtm atblclient](#), page B-89) from the command prompt.

The Startup Options dialog box appears, which you use to load a specific address-table file or create a new address table file.

The Startup Options dialog box contains options for loading or creating the address table data from:

| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New File        | <p>Opens the Address Table Properties dialog box, which you use to create a new address table file (see <a href="#">Creating a New Address Table File</a>, page 15-6). Create the new address table file.</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.</p>                                                                                                  |
| From File       | <p>Opens the Load File Dialog: Address Table File list, which you use to load a specific address table file and change the list of address table files (see <a href="#">Loading an Existing Address Table File</a>, page 15-8). Select an address table file to load.</p>                                                                                                                                                                                              |
| From ITP        | <p>Opens the Load Address Table from ITP wizard, which you use to select the ITP release 12.2(25)SW3 or later signaling point whose address table file you want to edit (see <a href="#">Loading an Address Table File from a Node</a>, page 15-10). Select a signaling point.</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.</p>                                  |
| From Archive    | <p>Opens the Load Address Table from Archive wizard, which you use to select the ITP release 12.2(25)SW3 or later node and signaling point whose address table file you want to edit (see <a href="#">Loading an Address Table File from the Archive</a>, page 15-12). Select a signaling point and table type.</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.</p> |

Once you close the Startup Options dialog box by creating a new address table file or loading an existing address table file, the Address Table Editor window appears. If you have created a new address table file, the table will be blank. If you have opened an existing address table file, the table will be populated.

**Figure 15-1**      **Address Table Editor Window**

## Address Table Menu

The menu on the Address Table Editor window contains:

| Menu Command                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > New Table<br>(Ctrl-N)             | <p>Opens the Address Table Properties dialog box. The MWTM prompts you to:</p> <ul style="list-style-type: none"><li>• Enter the table name, variant, instance number, and network name, then click <b>OK</b> to create the address table file.</li><li>• Click <b>Cancel</b> to close the prompt window without creating an address table file.</li></ul> <p>For more information, see <a href="#">Creating a New Address Table File, page 15-6</a>.</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.</p> |
| File > Load > Load From File<br>(Ctrl-L) | <p>Opens the Load File dialog box, allowing you to load an already existing address table file. The MWTM prompts you to:</p> <ul style="list-style-type: none"><li>• Select the file from the list, then click <b>OK</b> to load the address table file.</li><li>• Click <b>Cancel</b> to close the prompt window without loading an address table file.</li></ul> <p>For more information, see <a href="#">Loading an Existing Address Table File, page 15-8</a>.</p>                                                                                                                                            |

| Menu Command                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > Load > Load From Node<br>(Ctrl-T)    | <p>Opens the Load Address Table from ITP Wizard, which you use to select the ITP release 12.2(25)SW3 or later signaling point whose address table file you want to edit, as well as the table type.</p> <p><b>Tip</b> Click <b>Show Log</b> at any time to view the process details.</p> <p>To load the address table from a node:</p> <ol style="list-style-type: none"> <li>1. Select a node and signaling point from the drop-down list boxes, then click <b>Next</b> to load the address table list.</li> <li>2. Select an address table list from the drop-down list box, then click <b>Next</b> to enter your passwords.</li> <li>3. Enter the login password, then click <b>Next</b>.</li> <li>4. Enter the enable password, then click <b>Next</b>.</li> <li>5. Click <b>Finish</b> to complete the loading process.</li> </ol> <p>If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.</p> <p>For more information, see <a href="#">Loading an Address Table File from a Node, page 15-10</a>.</p> |
| File > Load > Load From Archive<br>(Ctrl-H) | <p>Opens the Load Address Table from Archive Wizard, which you use to select the ITP release 12.2(25)SW3 or later node and signaling point whose address table file you want to edit.</p> <p>To load the address from archive:</p> <ol style="list-style-type: none"> <li>1. Select a node and signaling point from the drop-down list boxes, then click <b>Next</b> to load the address table list.</li> <li>2. Select the address table list from the drop-down list box, then click <b>Next</b> to enter your passwords.</li> <li>3. Select the version from the table by clicking on it, then click <b>Next</b>.</li> <li>4. Click <b>Finish</b> to complete the loading process.</li> </ol> <p>If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.</p> <p>For more information, see <a href="#">Loading an Address Table File from the Archive, page 15-12</a>.</p>                                                                                                                                   |
| File > Revert<br>(Ctrl-R)                   | Reverts to the last saved version of the address table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| File > Save<br>(Ctrl-S)                     | Saves the changes that you make to the address table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| File > Save As                              | Opens the Save File Dialog: Address Table File list, which you use to save the address table file with a new name or overwrite an existing address table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Menu Command                                | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > Semantic Check<br>(Ctrl-K)           | Opens the Semantic Check address table dialog box, which you use to check the semantics of an address table file against a specific ITP (see <a href="#">Checking the Semantics of an Address Table File, page 15-17</a> ).                                                                                                                                                                                           |
| File > Deploy<br>(Ctrl-Y)                   | <p>Opens the Deployment wizard, which you use to validate an address table file, upload it to an ITP, and activate it on the ITP.</p> <p><b>Note</b> If you have not saved the current address table file, the Save File Dialog: Address Table File List appears, prompting you to save the file before continuing.</p> <p>For more information, see <a href="#">Deploying an Address Table File, page 15-18</a>.</p> |
| File > Exit<br>(Ctrl-Q)                     | <p>Closes the Address Table Editor window. The MWTM prompts you to confirm this action. Ensure that you save any changes before exiting, if necessary. Click:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b> to exit.</li> <li>• <b>No</b> to close the window.</li> </ul>                                                                                                                                   |
| Edit > Address Table Properties<br>(Ctrl-P) | Opens the Edit Address Table Properties dialog box, which you use to change the name, variant, version, instance ID, and network name associated with an address table file (see <a href="#">Editing Address Table Properties, page 15-17</a> ).                                                                                                                                                                      |
| Edit > Add<br>(Ctrl-E)                      | Adds a row to the address table.                                                                                                                                                                                                                                                                                                                                                                                      |
| Edit > Delete<br>(Ctrl-Delete)              | <p>Deletes one or more chosen rows from an address table. The Confirm Delete dialog box appears. To:</p> <ul style="list-style-type: none"> <li>• Delete the chosen rows, click <b>Yes</b>. The rows disappear from the table and the Confirm Delete dialog box closes.</li> <li>• Retain the chosen rows, click <b>No</b>. The rows remain in the table and the Confirm Delete dialog box closes.</li> </ul>         |
| Edit > Node Archive Management              | <p>Opens the Node Archive Management dialog box, which you use to view the contents of the archive, open a version with its corresponding editor, and delete all versions of a file (see <a href="#">Node Archive Management, page 5-33</a>).</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.</p>             |
| Edit > Node File Management                 | <p>Opens the Node File Management dialog box, which you use to transfer address table files to and from the ITP (see <a href="#">Node File Management, page 5-26</a>).</p> <p>If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.</p>                                                                                    |
| View > Address Table Info<br>(Ctrl-I)       | Opens the Address Table Information dialog box, which shows basic information about the currently visible address table file.                                                                                                                                                                                                                                                                                         |

| Menu Command                               | Description                                                                                                                                                     |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View > Network Name Configuration (Ctrl-F) | Opens the Network Name Configuration dialog box, which maps network names to variants and network indicators, in support of cross-instance address table files. |
| Help > Topics (F1)                         | Shows the table of contents for the MWTM online help.                                                                                                           |
| Help > Window (Shift-F1)                   | Shows online help for the current window.                                                                                                                       |
| Help > About (F3)                          | Shows build date, version, SSL support, and copyright information about the MWTM application.                                                                   |

## Creating a New Address Table File

You use the MWTM to create a new address table file. If you:

- Launch the Address Table Editor from the Startup Options window, click **New File**.
- Are already in the Address Table Editor, choose **File > New Table** from the Address Table Editor menu. You are prompted to save changes if you are currently working on an unsaved file.



### Note

If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

The Address Table Properties dialog box appears.

| Field or Button | Description                                                                                                                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Table Name      | User-defined unique table name.                                                                                                                                                                                                                                                  |
| Variant         | SS7 protocol variant. Select a variant from the drop-down list box. Valid variants are: <ul style="list-style-type: none"> <li>• ANSI</li> <li>• China</li> <li>• ITU</li> <li>• NTT</li> <li>• TTC</li> </ul>                                                                   |
| Version         | Version of the file format that the address table uses. Choose either: <ul style="list-style-type: none"> <li>• 1.1—Available beginning with 12.2(25)SW4a or 12.2(18)IXA</li> <li>• 1.3—Available beginning with 12.2(25)SW9, 12.2(18)IXC, 12.4(11)SW, or 12.2(33)IRA</li> </ul> |
| Instance Number | Number of the instance that the address table uses. Select an instance number from the drop-down list box. Valid numbers are <b>0</b> to <b>7</b> . The default instance number is <b>0</b> .                                                                                    |



| Field or Button | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Name    | <p>Network name that the address table uses. Select a network name from the drop-down list box. When you select the network name, the MWTM automatically sets the corresponding variant in the Variant field.</p> <p>If you change the network name for an existing address table file, the new network name must use the same variant.</p> |
| OK              | <p>Creates the new address table file and closes the Address Table Properties dialog box.</p> <p>Enter or select values for the new address table file, then click <b>OK</b>. The MWTM creates the new address table file and closes the Address Table Properties dialog box.</p>                                                           |
| Cancel          | <p>Closes the Address Table Properties dialog box without creating a new address table file.</p> <p>To close the Address Table Properties dialog box without creating a new address table file, click <b>Cancel</b>.</p>                                                                                                                    |
| Help            | <p>Shows online help for the current window.</p>                                                                                                                                                                                                                                                                                            |

**Related Topics:**

- [Loading an Existing Address Table File, page 15-8](#)
- [Loading an Address Table File from a Node, page 15-10](#)

## Loading an Existing Address Table File

You use the MWTM to load a specific address table file and change the list of address table files. If you:

- Launch the Address Table Editor from the Startup Options window, click **From File**.
- Are already in the Address Table Editor, choose **File > Load > Load From File** from the Address Table Editor menu. You are prompted to save changes if you are currently working on an unsaved file.



### Note

When you load an address table file, the name of the server that is associated with the address table client and the filename, as well as the table type and mode (can be edit or view only), appear in the window name:

```
MWTM: Address Table Editor -- mwtm-sun8 -- address table.File.1 (MLR edit mode)
```

If you have not yet loaded or saved an address table file, the message `No File Loaded` appears in place of the address-table filename.

The Load File Dialog: Address Table File List appears.

| Field or Button                           | Description                                                          |
|-------------------------------------------|----------------------------------------------------------------------|
| File Types                                | Drop-down list only includes MLR.                                    |
| Type                                      | Icon indicating whether the item in the table is a file or a folder. |
| Name                                      | Name of the address table file or folder.                            |
| Last Modified                             | Date and time the address table file or folder was last modified.    |
| Size (bytes)                              | Size of the address table file or folder, in bytes.                  |
| Number of Files<br>(in lower-left corner) | Total number of address table files and folders.                     |

| Field or Button | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK              | <p>When you click this button, it:</p> <ul style="list-style-type: none"> <li>• Loads the chosen address table file.</li> <li>• Saves any changes you made to the list of files.</li> <li>• Closes the Load File Dialog: Address Table File list.</li> <li>• Opens the Progress dialog box</li> <li>• Begins loading the address table file.</li> </ul> <p>To load an address table file:</p> <ul style="list-style-type: none"> <li>• Double-click it in the list</li> <li>• Select it in the list and click <b>OK</b>. <ul style="list-style-type: none"> <li>– Or, enter the name of the file and click <b>OK</b>.</li> </ul> </li> </ul> <p>The MWTM closes the Load File Dialog: Address Table File list and the Progress dialog box appears, which shows the progress of the address table file load, as well as any messages that appear while loading the file.</p> <ul style="list-style-type: none"> <li>• When the file has been loaded, click <b>OK</b>.</li> </ul> <p>The MWTM closes the Progress dialog box, loads the address table file, and returns to the Address Table Editor window.</p> |
| Delete          | Deletes the chosen file from the address table file list. The MWTM issues an informational message containing the name and location of the deleted file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Cancel          | Closes the dialog box without loading an address table file or saving any changes to the address table file list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Help            | Shows online help for the dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Related Topics:**

- [Launching the Address Table Editor, page 15-2](#)
- [Loading an Address Table File from a Node, page 15-10](#)

# Loading an Address Table File from a Node

**Note**

Before using the Load Address Table From ITP wizard to load address table files, you must enable TFTP file transfer for the address table staging directory by using the **mwtm atbldir** command (see [mwtm atbldir](#), page B-90).

You use the Load Address Table From ITP wizard to load an existing address table file from a node. If you:

- Launch the Address Table Editor from the Startup Options window, click **From Node**.
- Are already in the Address Table Editor, choose **File > Load > Load From Node** from the Address Table Editor menu.

If you implement MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

The Load Address Table From ITP wizard appears.

**Figure 15-2**      *Load Address Table From ITP Wizard*

The left pane of the Load Address Table From ITP wizard contains:

| Step           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Node/SP | <p>You can select the signaling point from which the address table should be loaded. You can optionally check the <b>Filter by Node</b> check box, which limits signaling point selection to a specific node.</p> <p>Select a signaling point and node (optional) from the drop-down list boxes, then click <b>Next</b> . The MWTM retrieves address table names from the chosen signaling point.</p> <p>If no address table names are available, the process ends with errors. If address table names are available, the MWTM proceeds directly to the Select Table step.</p> |
| Login          | <p>You can log in to the ITP. Enter the:</p> <ul style="list-style-type: none"> <li>• Log in password, if required.</li> <li>• Enable password, if required.</li> </ul> <p><b>Note</b> To avoid entering user name and password information each time, you can set up credentials (see <a href="#">Configuring Login Credentials, page 3-20</a>).</p>                                                                                                                                                                                                                          |
| Load           | <p>Uploads the address table file to the MWTM.</p> <p>If the file upload ends with no errors, the process is successful. Click <b>Finish</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                              |

The bottom line of the Load Address Table From ITP wizard contains:

| Field or Button   | Description                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Progress Bar      | Indicates that the address table file is being uploaded.                                                                                                           |
| Show Log/Hide Log | Shows or hides the log file for the Load Address Table From ITP wizard.                                                                                            |
| Next >            | Advances to the next step in the Load Address Table From ITP wizard.                                                                                               |
| Finish            | Closes the Load Address Table From ITP wizard. The Finish button appears when loading ends successfully or the wizard detects errors and the process is cancelled. |
| Cancel            | Closes the Load Address Table From ITP wizard without loading the file.                                                                                            |
| Help              | Shows online help for the Load Address Table From ITP wizard.                                                                                                      |

#### Related Topics:

- [Launching the Address Table Editor, page 15-2](#)
- [Loading an Existing Address Table File, page 15-8](#)
- [Editing Address Table Properties, page 15-17](#)

# Loading an Address Table File from the Archive



## Note

Before using the Load Address Table From Archive wizard to load address table files, you must use the **mwtm atbldir** command to enable TFTP file transfer for the address table staging directory (see [mwtm atbldir](#), page B-90).

You can use the Load Address Table From Archive wizard to load an existing address table file from the archive. If you:

- Launch the Address Table Editor, from the Startup Options window, click **From Archive**.
- Are already in the Address Table Editor, choose **File > Load > Load From Archive** from the Address Table Editor menu.

If you implement MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

The Load Address Table From Archive wizard appears.

**Figure 15-3 Load Address Table From Archive Wizard**



*We need to re-capture this screen, I could not re-create.*

The left pane of the Load Address Table From Archive wizard contains:

| Step           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Node/SP | <p>You can select the signaling point from which to load the address table. You can optionally check the <b>Filter by Node</b> check box, which limits signaling point selection to a specific node.</p> <p>Select a signaling point and node (optional) from the drop-down list boxes, then click <b>Next</b>. The MWTM retrieves address table names from the chosen signaling point.</p> <p>If no address table names are available, the process completes with errors. If address table names are available, the MWTM proceeds directly to the Select Table step.</p> |
| Select Version | <p>You can select the version you want to load. Click a version to highlight it, then click <b>Next</b>. The table contains:</p> <ul style="list-style-type: none"> <li>• <b>Rev</b>—Revision number.</li> <li>• <b>Date</b>—Date and time the version was created.</li> <li>• <b>Comments</b>—Provided at the time of creation, if applicable.</li> <li>• <b>Author</b>—Initiator of the comments.</li> </ul>                                                                                                                                                            |
| Load           | <p>Uploads the address table file to the MWTM.</p> <p>If the file upload ends with no errors, the process is successful. Click <b>Finish</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |

The bottom line of the Load Address Table From Archive wizard contains:

| Field or Button | Description                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Progress Bar    | Indicates that the address table file is being uploaded.                                                                                                        |
| Next >          | Advances to the next step in the Load Address Table From ITP wizard.                                                                                            |
| Finish          | Closes the Load Address Table From ITP wizard. The Finish button appears when loading completes successfully or it detects errors and the process is cancelled. |
| Cancel          | Closes the Load Address Table From ITP wizard without loading the file.                                                                                         |
| Help            | Shows online help for the Load Address Table From ITP wizard.                                                                                                   |

#### Related Topics:

- [Launching the Address Table Editor, page 15-2](#)
- [Loading an Existing Address Table File, page 15-8](#)
- [Loading an Address Table File from a Node, page 15-10](#)
- [Editing Address Table Properties, page 15-17](#)

## Working in Address Table Files

Once you create a new address table file or load an existing address table file, you can manage the address table entries.

If you implement MWTM User-Based Access, these options are available to users with authentication level Network Administrator (level 4) and higher. To:

- Add a row to a table, select the table and choose **Edit > Add** from the address table menu; or, **Add** from the right-click menu.
- Delete one or more rows from a table, select the rows and choose **Edit > Delete** from the address table menu; or, **Delete** from the right-click menu.
- Edit the values in each row in each table, type over the current value or select a new value from a drop-down list box. If you are editing a row, you cannot move on until all fields in the row are completed.
- Reset a cell to its previous value. Press **Esc**. Press **Esc** twice to reset the entire row.
- Commit your changes, click outside the row or press **Enter**.



**Note** Once you commit your changes, pressing **Esc** does not reset the cells in the row.

The Address Table Editor window contains:

| Heading        | Description                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| Address Digits | Address digits for the address table. Enter a 1- to 20-digit hexadecimal string. The value must be unique in an address table. |
| Exact Match    | Considers the address an exact match.                                                                                          |
| Result Type    | Type of action to perform on a match.                                                                                          |
| Result Value   | Values to use with the matching action.                                                                                        |



## Result Types and Values

This table defines the list of result types from which to choose when you click in the Result Types column and the drop-down arrow that appears, also the corresponding result values that you enter for MLR address tables:

| Result Type | Result Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Description                                                                   |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| asname      | Route to the specified application server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Message is routed to a particular destination M3UA or SUA application server. |
| block       | (Optional, version 1.3 only)<br>The Edit SCCP Error window appears. Enter a value: <ul style="list-style-type: none"> <li>• 0—No data for TT</li> <li>• 1—No translation for address</li> <li>• 2—Subsystem congestion</li> <li>• 3—Subsystem is failed</li> <li>• 4—Subsystem is unequipped</li> <li>• 5—SS7 network failure</li> <li>• 6—SS7 network congestion</li> <li>• 7—Unqualified</li> <li>• 8—XUDTS error in message transport</li> <li>• 9—XUDTS error in local processing</li> <li>• A—XUDTS cannot perform reassembly</li> <li>• B—SCCP failure</li> <li>• C—SCCP hop counter violation</li> <li>• D—Segmentation not supported</li> <li>• E—Segmentation failure</li> <li>• WORD ITU SCCP Spare Error Codes in Hex {F..FF}</li> </ul> Click <b>Add</b> to accept the value. | Indicates that you should discard the short message.                          |
| continue    | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Message that the normal SCCP routing will process the message.                |
| group       | Specify the name of the result group to which to route.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Indicates that a result group is used for routing.                            |

| Result Type | Result Value                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| gt          | <SCCP address> <b>tt</b> <number><br><b>gti</b> <number> | <p>Indicates that the message is routed by using SCCP global title. Places the specified address in the SCCP Called Party Address. The routing indicator changes to <b>RI=GT</b>. Then routed based on the locally provisioned global-title translation table. When you select this parameter and click the corresponding space in the Result Value column, the Edit GTT dialog box appears and contains:</p> <ul style="list-style-type: none"> <li>• <b>SCCP Address</b>—An address string of 1-15 hexadecimal characters. The string is not input in BCD-String format, but in normal form.</li> <li>• <b>Translation Type</b>—Identifies the translation type that the address specifies. Valid values are 0-255.</li> <li>• <b>Global Title Indicator</b>—Identifies the global title indicator value for the specified address. This value is always <b>2</b> for an ANSI variant and might be 2 or 4 for other variant types.</li> <li>• <b>Numbering Plan</b>—Identifies the numbering plan of the specified address. This value is only specified when the <b>gti</b> parameter value is 4. Valid values are 0-15.</li> <li>• <b>Nature of Address Indicator</b>—Identifies the nature of the specified address. This value is only specified when the <b>gti</b> parameter value is 4. Valid values are 0-127.</li> <li>• <b>Add</b>—Adds the current values.</li> <li>• <b>Close</b>—Closes the dialog box.</li> <li>• <b>Help</b>—Launches the online help window for the current dialog box.</li> </ul> |
| none        | none                                                     | A result is not specified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| pc          | <point code> <b>ssn</b> <number>                         | <p>Indicates that <b>pc</b> or <b>pc/ssn</b> routing is used. When you select this parameter and click the corresponding space in the Result Value column, the Edit Point Code dialog box appears and displays these fields and buttons:</p> <ul style="list-style-type: none"> <li>• <b>Point Code</b>—Point code to route the message.</li> <li>• <b>SSN</b>—Specify a subsystem number. Valid values are 2-255.</li> <li>• <b>Add</b>—Adds the current values.</li> <li>• <b>Close</b>—Closes the dialog box.</li> <li>• <b>Help</b>—Launches the online help window for the current dialog box.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Editing Address Table Properties

You can use the MWTM to edit the address table properties associated with an address table file. Choose **Edit > Address Table Properties** from the Address Table Editor menu. The Edit Address Table Properties dialog box appears.

| Field or Button | Description                                                                                                                                                                                                                                                    |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Table Name      | User-defined unique table name.                                                                                                                                                                                                                                |
| Variant         | SS7 protocol variant. You cannot edit this field.                                                                                                                                                                                                              |
| Version         | Version of the file format that the address table uses. You cannot edit this field.                                                                                                                                                                            |
| Instance Number | Number of the instance that the address table uses. Valid numbers are <b>0</b> to <b>7</b> ; the default instance number is <b>0</b> .                                                                                                                         |
| Network Name    | Network name that the address table uses.<br><br>If you change the network name for an existing address table file, the new network name must use the same variant.                                                                                            |
| OK              | Saves the changes to the address table file.<br><br>Enter or select values, then click <b>OK</b> . The MWTM saves your changes to the address table file.                                                                                                      |
| Cancel          | Closes the Edit Address Table Properties dialog box without saving any changes to the address table file.<br><br>To close the Edit Address Table Properties dialog box at any time without saving any changes to the address table file, click <b>Cancel</b> . |
| Help            | Shows online help for the current window.                                                                                                                                                                                                                      |

## Checking the Semantics of an Address Table File

In using the MWTM, Cisco strongly recommends that you check the semantics of an address table file against a specific ITP, validating these data in the address table file:

**Group Name**—In the Address Table entries, when the result type is *group* the result value is a group name. You must configure the group name in the address entry on the ITP prior to the deployment of the address table. During the validation process, if the group name in the address entry does not have a corresponding match on the ITP, the MWTM generates an error.

To check the semantics of an address table file, choose **File > Semantic Check** from the Address Table Editor menu. The Semantic Check address table dialog box appears.

| Field or Button        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ITP Name or IP Address | Name or IP address of the ITP against which to check the address table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| OK                     | <p>Closes the Semantic Check Address Table dialog box and opens the Progress dialog box, which shows the progress of the semantic check for the address table file.</p> <p>Enter the name or IP address of an ITP, and click <b>OK</b>. The the Semantic Check Address Table dialog box closes and the Progress dialog box opens, which shows the progress of the semantic check for the address table file and any messages that appear while checking the file.</p> <p>When the check ends, click <b>OK</b>. The Progress dialog box closes and returns to the Semantic Check Address Table dialog box.</p> |
| Cancel                 | Closes the Semantic Check Address Table dialog Box without checking the semantics of the address table file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Note**

You can also use the **mwtm checkmlr** command to check the semantics of an MLR address table file (see [mwtm checkmlr](#), page B-92).

## Deploying an Address Table File

You use the Deployment wizard to validate an address table file, upload it to an ITP, archive the file, and activate it on the ITP. To launch the Deployment wizard for an address table file, use one of these procedures:

- Choose **File > Deploy** from the Address Table Editor menu (see [Deploying ITP Files](#), page 5-36).
- Enter the **mwtm pushmlr** command (see [mwtm pushmlr](#), page B-109).

## Displaying Basic Information About an Address Table File

You use the MWTM to view basic information about the current address table file. Choose **View > Address Table Info** from the address table menu. The Address Table Information dialog box appears.

The Address Table Information dialog box is read-only.

| Field or Button | Description                                                                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Table Name      | User-defined unique table name.                                                                                                                            |
| Filename        | Name of the address table file.                                                                                                                            |
| Version         | Version of the file format that the address table uses.                                                                                                    |
| Variant         | SS7 protocol variant. Valid variants are: <ul style="list-style-type: none"><li>• ANSI</li><li>• China</li><li>• ITU</li><li>• NTT</li><li>• TTC</li></ul> |
| Network Name    | Network name that the address table file uses.                                                                                                             |
| Instance Number | Number of the instance that the address table uses. Valid numbers are 0 to 7. The default instance number is 0.                                            |
| Last Modified   | Date and time that someone last modified the address table file.                                                                                           |
| Total Entries   | Total number of entries in the address table file.                                                                                                         |
| OK              | Closes the address table Table Info dialog box.                                                                                                            |

## Listing Archived Address Tables

To view a list of deployed and archived MLR address tables, do one of the following:

- Enter the **mwtm listarchive** command (see [mwtm listarchive](#), page B-103).
- In the MWTM Address Table Editor, choose **Edit > Node Archive Management** (see [Node Archive Management](#), page 5-33).

For a list of current MLR address table files in the address table staging directory, enter the **mwtm listmlr** command (see [mwtm listmlr](#), page B-104).

## Creating Network Name Mapping Files

When the MWTM discovers your network, it automatically creates and populates the network name-mapping file; therefore, in most cases, you do not need to manually create the network name-mapping file. For more information about running Discovery, see [Discovering Your Network](#), page 4-4.

In some cases, you might want to manually create the network name-mapping file; for example, you might not have run **Discovery** yet, but you want to prepare for a future address table configuration. Also, while you cannot change or delete entries that have been populated automatically by the MWTM, you can add entries manually; and, you can change or delete those manual entries.

To create the network name-mapping file manually; or, add, change, or delete manual entries, choose **View > Network Name Configuration** from the address table menu. If you implement MWTM User-Based Access, this option is available to users with authentication level System Administrator (level 5). The Network Name Configuration dialog box appears.

The Network Name Configuration dialog box contains:

- [Network Name Configuration Dialog Menu](#), page 15-21
- [Network Name Configuration Dialog Table](#), page 15-22

## Network Name Configuration Dialog Menu

The menu on the Network Name Configuration dialog box contains:

| Menu Command                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File > Revert<br>(Ctrl-R)   | Loads the most recent network name-mapping file from the MWTM server.<br><br>If the MWTM discovers new entries for the network name-mapping file while you are editing an address table file (for example, if a new network instance is added, or a new network is discovered), the Address Table Editor does not detect the new entries and they do not appear in the Network Name Configuration dialog box. To see the new entries in the dialog box, choose <b>File &gt; Revert</b> . (You can also restart the Address Table Editor to automatically load the most recent network name-mapping file from the MWTM server.) |
| File > Save<br>(Ctrl-S)     | Saves the changes that you make to the network name-mapping file.<br><br>After you add, change, or delete entries and save the file, the MWTM uses the file the next time it discovers the network. However, if the MWTM discovers entries that conflict with manual entries in the file, the MWTM uses (and shows in the Network Name Configuration dialog box) the discovered entries; not the manual entries.                                                                                                                                                                                                               |
| File > Print<br>(Ctrl-P)    | Prints the contents of the network name-mapping file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| File > Close<br>(Ctrl-W)    | Closes the network name-mapping file without saving any additions, changes, or deletions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Edit > Add<br>(Alt-A)       | Adds an entry to the network name-mapping file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Edit > Delete<br>(Delete)   | Deletes the chosen entry from the network name-mapping file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Help > Topics<br>(F1)       | Shows the table of contents for the MWTM online help.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Help > Window<br>(Shift-F1) | Shows online help for the current window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Help > About<br>(F3)        | Shows build date, version, SSL support, and copyright information about the MWTM application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Network Name Configuration Dialog Table

The Network Name Configuration Dialog table contains:

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Name      | Network name that the address table file uses.<br><br>If you change the network name for an existing address table file, the new network name must use the same variant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Variant           | SS7 protocol variant. Valid variants are: <ul style="list-style-type: none"><li>• ANSI</li><li>• China</li><li>• ITU</li><li>• NTT</li><li>• TTC</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Network Indicator | Type of call that a user places. Valid values are: <ul style="list-style-type: none"><li>• <b>National</b>—National-bound call. The MWTM routes national calls through the national network.</li><li>• <b>NationalSpare</b>—National-bound call, used in countries in which more than one carrier can share a point code. In those countries, the Network Indicator differentiates networks.</li><li>• <b>International</b>—International-bound call. The MWTM forwards international-bound calls to an STP pair that acts as an international gateway.</li><li>• <b>InternationalSpare</b>—International-bound call, used in countries in which more than one carrier can share a point code. In those countries, networks are differentiated by the Network Indicator.</li></ul> |
| Discovered        | Indicates whether the: <ul style="list-style-type: none"><li>• MWTM (Yes) discovered the entry.</li><li>• A user entered it manually (No).</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |



## Saving an Address Table File

You use the MWTM to save a specific address table file and change the list of address table files.

If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

To save the changes that you make to an address table file or change the list of address table files, use one of these procedures. To save the changes that you make to the address table file:

- Without changing the name of the file, choose **File > Save** from the address table menu.
- With a new name, choose **File > Save As** from the address table menu. The Save File Dialog: Address Table File List appears.

| Field or Button or Icon                            | Description                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                                               | Icon indicating whether the item in the table is a file or a folder.                                                                                                                                                                                                                                                                                                    |
| Name                                               | Name of the address table file or folder.                                                                                                                                                                                                                                                                                                                               |
| Last Modified                                      | Date and time a user last modified the address table file or folder.                                                                                                                                                                                                                                                                                                    |
| Size (bytes)                                       | Size of the address table file or folder, in bytes.                                                                                                                                                                                                                                                                                                                     |
| Filename                                           | Name by which you want to save the address table file.<br><br>If you create a new address table filename, you can use any letters, numbers, or characters in the name that your operating system allows. However, if you include spaces in the new name, the MWTM converts those spaces to hyphens (-); for example, the MWTM saves file <i>a b c</i> as <i>a-b-c</i> . |
| Number of Files<br>(visible in bottom left corner) | Total number of address table files and folders.                                                                                                                                                                                                                                                                                                                        |

| Field or Button or Icon | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OK                      | <p>Saves the address table file or any changes you made to the list of files and closes the dialog box.</p> <p>To save the address table file with a new name, use one of these procedures. To save the file with:</p> <ul style="list-style-type: none"> <li>A completely new name, enter the new name and click <b>OK</b>.</li> <li>An existing name, overwriting an old address table file, select the name in the list and click <b>OK</b>.</li> </ul> <p>The MWTM closes the Save File Dialog: Address Table File List and the Progress dialog box appears, which shows the progress of the address table file save, as well as any messages that appear while saving the file.</p> <p>When the file is saved, click <b>OK</b>. The MWTM:</p> <ul style="list-style-type: none"> <li>Closes the Progress dialog box.</li> <li>Saves the address table file with the new name</li> <li>Returns to the Address Table Editor window.</li> </ul> <p><b>Note</b> If another user modifies and saves the address table file before you save your changes, the MWTM asks if you want to overwrite that user's changes. If you do, the other user's changes are overwritten and lost. If you choose not to, your changes are lost; unless you save the address table file to a different filename.</p> |
| Delete                  | Deletes the chosentur file from the address table file list. The MWTM issues an informational message containing the name and location of the deleted file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cancel                  | Closes the dialog box without saving the address table file or any changes to the address table file list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Help                    | Shows online help for the dialog box.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

When you are ready to exit the Address Table Editor window, choose **File > Exit** from the address table menu.

If you made any changes to the address table file, the MWTM asks if you want to save the changes before leaving the window. Click:

- Yes** to save the changes.

The MWTM opens the Save File Dialog: Address Table File List, which you use to save the address table file with a new name, or overwrite an existing address table file.

- No** to close the prompt window.

The MWTM closes the Address Table Editor window without saving any changes to the address table file.

By default, address table files reside in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the default directory is */opt/CSCOsgm/atbl*.
- A different directory, then the default directory resides in that directory.

To change the directory in which the MWTM stores address table files, use the **mwtm atbldir** command (see [mwtm atbldir](#), page B-90).

## Reverting to the Last Saved Address Table File

To revert to the last saved version of the address table file, choose **File > Revert** from the address table menu. The MWTM shows the last saved version of the file.

If you implement MWTM User-Based Access, this option is available to users with authentication level Network Administrator (level 4) and higher.

■   Reverting to the Last Saved Address Table File



# APPENDIX A

## Client Object Map Reference

In the Mobile Wireless Transport Manager (MWTM) client navigation tree, if you click on an object in a view, the associated tabs appear in the content area in the right pane. This appendix provides an overview of the tabs available for each MWTM object in a view, and contains:



### Note

The MWTM web interface may contain additional tabs (for details, see [Chapter 11, “Accessing Data from the Web Interface.”](#))

| Object Type | Related Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Applicable To |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Nodes       | <ul style="list-style-type: none"><li>• <a href="#">BWG Node Tabs, page A-2</a></li><li>• <a href="#">CSG1 and CSG2 Node Tabs, page A-3</a></li><li>• <a href="#">CSR Node Tabs, page A-3</a></li><li>• <a href="#">GGSN Node Tabs, page A-4</a></li><li>• <a href="#">HA Node Tabs, page A-4</a></li><li>• <a href="#">IP-RAN Node Tabs, page A-5</a></li><li>• <a href="#">ITP Node Tabs, page A-5</a></li><li>• <a href="#">mSEF Node Tabs, page A-6</a></li><li>• <a href="#">ONS Node Tabs, page A-6</a></li><li>• <a href="#">RAN Service Card Node Tabs, page A-7</a></li><li>• <a href="#">Unknown Node Tabs, page A-7</a></li></ul> | All networks  |

| Object Type                             | Related Content                                                          | Applicable To       |
|-----------------------------------------|--------------------------------------------------------------------------|---------------------|
| Signaling Points                        | <a href="#">Signaling Point Tabs, page A-8</a>                           | ITP networks only   |
| Linksets                                | <a href="#">Linkset Tabs, page A-9</a>                                   |                     |
| Links                                   | <a href="#">Link Tabs, page A-9</a>                                      |                     |
| Application Servers                     | <a href="#">Application Server Tabs, page A-9</a>                        |                     |
| Application Server Processes            | <a href="#">Application Server Process Tabs, page A-10</a>               |                     |
| Application Server Process Associations | <a href="#">Application Server Process Association Tabs, page A-10</a>   |                     |
| Signaling Gateway-Mated Pairs           | <a href="#">Signaling Gateway-Mated Pair Tabs, page A-11</a>             |                     |
| Interfaces                              | <a href="#">Interface Tabs, page A-11</a>                                | All networks        |
| RAN Shorthauls                          | <a href="#">UMTS and GSM Interface Tabs, page A-12</a>                   | RAN-O networks only |
| Cards                                   | <a href="#">Card Tabs, page A-12</a>                                     |                     |
| RAN Backhauls                           | <a href="#">RAN Backhaul Tabs, page A-13</a>                             |                     |
| Folders                                 | <a href="#">Physical and Management Interface Folder Tabs, page A-13</a> | All networks        |
| Access Point Name (APN)                 | <a href="#">GGSN Node Tabs, page A-4</a>                                 | GGSN networks only  |

## BWG Node Tabs

Clicking a Broadband Wireless Gateway (BWG) node in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance         | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog              | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



### Note

To view all nodes in your system, see [Nodes Table, page 6-5](#).

# CSG1 and CSG2 Node Tabs

Clicking a CSG node in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance         | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog              | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



## Note

To view all nodes in your system, see [Nodes Table, page 6-5](#).

# CSR Node Tabs

Clicking a Cell Site Router (CSR) node in a MWTM view may provide you with these tabs:

| Tab                                                                          | Related Content                                             |
|------------------------------------------------------------------------------|-------------------------------------------------------------|
| Alarms                                                                       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details                                                                      | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes                                                                        | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance                                                                  | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| PWE3 Statistics                                                              | <a href="#">Viewing PWE3 Statistics, page 8-121</a>         |
| <b>Note</b> This tab is only available for CSR nodes operating Pseudo Wires. |                                                             |
| Recent Events                                                                | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors                                                          | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog                                                                       | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Trap Settings                                                                | <a href="#">Viewing Trap Settings, page 8-62</a>            |
| Troubleshooting                                                              | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



## Note

To view all nodes in your system, see [Nodes Table, page 6-5](#).

## GGSN Node Tabs

Clicking a GGSN node in a MWTM view may provide you with these tabs:

| Tab                                                       | Related Content                                             |
|-----------------------------------------------------------|-------------------------------------------------------------|
| Alarms                                                    | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details                                                   | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes                                                     | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance                                               | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| Recent Events                                             | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors                                       | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog                                                    | <a href="#">Viewing the Syslog, page 8-57</a>               |
| <b>Note</b> The syslog tab is only available for GGSN R8. |                                                             |
| Troubleshooting                                           | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



### Note

To view all nodes in your system, see [Nodes Table, page 6-5](#).

## HA Node Tabs

Clicking an HA node in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance         | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog              | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



### Note

To view all nodes in your system, see [Nodes Table, page 6-5](#).



# IP-RAN Node Tabs

|                     |                                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance         | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| PWE3 Statistics     | <a href="#">Viewing PWE3 Statistics, page 8-121</a>         |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog              | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



## Note

To view all nodes in your system, see [Nodes Table, page 6-5](#).

# ITP Node Tabs

Clicking an IP Transfer Point (ITP) node in a MWTM view may provide you with these tabs:

| Tab                                                                                               | Related Content                                             |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Alarms                                                                                            | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details                                                                                           | <a href="#">Viewing Details, page 8-12</a>                  |
| MSU Rates                                                                                         | <a href="#">Viewing ITP MSU Rates, page 8-94</a>            |
| <b>Note</b> Only available for ITPs that have an IOS that implements the CISCO-ITP-MSU-RATES-MIB. |                                                             |
| MTP3 Errors                                                                                       | <a href="#">Viewing ITP MTP3 Errors, page 8-93</a>          |
| Non-Stop Operation                                                                                | <a href="#">Viewing ITP Non-Stop Operation, page 8-95</a>   |
| <b>Note</b> Only available for ITPs with the NSO feature; 7500 or 7600 devices.                   |                                                             |
| Notes                                                                                             | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance                                                                                       | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| Recent Events                                                                                     | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors                                                                               | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog                                                                                            | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Trap Settings                                                                                     | <a href="#">Viewing Trap Settings, page 8-62</a>            |
| Troubleshooting                                                                                   | <a href="#">Viewing Troubleshooting, page 8-43</a>          |

**Note**

To view all nodes in your system, see [Nodes Table, page 6-5](#).

## mSEF Node Tabs

This is a 7600 supervisor card in a chassis that contains SAMI cards.

|                     |                                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance         | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog              | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |

**Note**

To view all nodes in your system, see [Nodes Table, page 6-5](#).

## ONS Node Tabs

Clicking an Optical Networking System (ONS) node in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |

**Note**

To view all nodes in your system, see [Nodes Table, page 6-5](#).

# RAN Service Card Node Tabs

Clicking a Radio Access Network (RAN) Service Card (SVC) node in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Performance         | <a href="#">Viewing CPU Performance, page 8-58</a>          |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Syslog              | <a href="#">Viewing the Syslog, page 8-57</a>               |
| Trap Settings       | <a href="#">Viewing Trap Settings, page 8-62</a>            |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |

**Note**

To view all nodes in your system, see [Nodes Table, page 6-5](#).

## CDT Node Tabs

Clicking a CDT node tab may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |

**Note**

To view all nodes in your system, see [Nodes Table, page 6-5](#).

## Unknown Node Tabs

**Note**

Unknown nodes will show a performance tab when the unknown node implements the CISCO-PROCESS-MIB and either the CISCO-ENHANCED-MEMPOOL-MIB or CISCO-MEMORY-POOL-MIB.

Clicking a node in a MWTM view with unknown node status may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |

**Note**

To view all nodes in your system, see [Nodes Table, page 6-5](#).

## Signaling Point Tabs

Clicking on a signaling point in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| GTT MAP Status      | <a href="#">Viewing GTT MAP Status, page 8-125</a>          |
| GTT Statistics      | <a href="#">Viewing GTT Statistics, page 8-126</a>          |
| ITP Access Lists    | <a href="#">Viewing Route Detail, page 8-124</a>            |
| MLR Details         | <a href="#">Viewing MLR Details, page 8-130</a>             |
| MTP3 Event Log      | <a href="#">Viewing the MTP3 Event Log, page 8-129</a>      |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Route Detail        | <a href="#">Viewing Route Detail, page 8-124</a>            |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |

**Note**

To view all signaling points in your system, see [Signaling Points Table, page 6-8](#).

# Linkset Tabs

Clicking on a linkset in a MWTM view may provide you with these tabs:

| Tab                  | Related Content                                              |
|----------------------|--------------------------------------------------------------|
| Alarms               | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>  |
| Details              | <a href="#">Viewing Details, page 8-12</a>                   |
| Linkset Access Lists | <a href="#">Viewing ITP Linkset Access Lists, page 8-123</a> |
| Notes                | <a href="#">Viewing Notes, page 6-39</a>                     |
| Recent Events        | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>  |
| Status Contributors  | <a href="#">Viewing Status Contributors, page 8-10</a>       |
| Troubleshooting      | <a href="#">Viewing Troubleshooting, page 8-43</a>           |



## Note

To view all linksets in your system, see [Linksets Table, page 6-10](#).

# Link Tabs

Clicking on a link in a MWTM view may provide you with these tabs:

| Tab             | Related Content                                             |
|-----------------|-------------------------------------------------------------|
| Alarms          | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details         | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes           | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events   | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Troubleshooting | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



## Note

To view all links in your system, see [Links Table, page 6-13](#).

# Application Server Tabs

Clicking on an application server in a MWTM view may provide you with these tabs:

| Tab           | Related Content                                             |
|---------------|-------------------------------------------------------------|
| Details       | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes         | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |

| Tab                 | Related Content                                        |
|---------------------|--------------------------------------------------------|
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a> |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>     |

**Note**

To view all application servers in your system, see [Application Servers Table, page 6-14](#).

## Application Server Process Tabs

Clicking on an application server process in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| Troubleshooting     | <a href="#">Viewing Troubleshooting, page 8-43</a>          |

**Note**

To view all application server processes in your system, see [Application Server Processes Table, page 6-16](#).

## Application Server Process Association Tabs

Clicking on an application server process association in a MWTM view may provide you with these tabs:

| Tab             | Related Content                                             |
|-----------------|-------------------------------------------------------------|
| Alarms          | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details         | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes           | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events   | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Troubleshooting | <a href="#">Viewing Troubleshooting, page 8-43</a>          |

**Note**

To view all application server process associations in your system, see [Application Server Process Associations Table, page 6-18](#).

# Signaling Gateway-Mated Pair Tabs

Clicking on a signaling gateway-mated pair in a MWTM view may provide you with these tabs:

| Tab             | Related Content                                             |
|-----------------|-------------------------------------------------------------|
| Alarms          | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details         | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes           | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events   | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Troubleshooting | <a href="#">Viewing Troubleshooting, page 8-43</a>          |



## Note

To view all signaling gateway-mated pairs in your system, see [Signaling Gateway Mated Pairs Table, page 6-19](#).

# Interface Tabs

Clicking on an interface in a MWTM view may provide you with these tabs:

| Tab                                                                                                                                   | Related Content                                             |
|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Alarms                                                                                                                                | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details                                                                                                                               | <a href="#">Viewing Details, page 8-12</a>                  |
| Interface Errors <sup>1</sup>                                                                                                         | <a href="#">Viewing Data for Interfaces, page 8-63</a>      |
| Interface Performance <sup>2</sup>                                                                                                    | <a href="#">Viewing Data for Interfaces, page 8-63</a>      |
| Notes                                                                                                                                 | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events                                                                                                                         | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors <sup>3</sup>                                                                                                      | <a href="#">Viewing Status Contributors, page 8-10</a>      |
| TDM Statistics                                                                                                                        | <a href="#">Viewing TDM Statistics, page 8-103</a>          |
| <b>Note</b> TDM statistics are available only on some interfaces on nodes that implement either the CISCO-ICSUDSU-MIB or RFC1406-MIB. |                                                             |
| Troubleshooting                                                                                                                       | <a href="#">Viewing Troubleshooting, page 8-43</a>          |

1. May not be applicable for interfaces that do not collect statistics.
2. May not be applicable for interfaces that do not collect statistics.
3. May not show for parent interfaces that have no children.



## Note

To view all interfaces in your system, see [Interfaces Table, page 6-21](#).

# UMTS and GSM Interface Tabs

Clicking on a RAN shorthaul (either UMTS or GSM) in a MWTM view may provide you with these tabs:

| Tab                   | Related Content                                                |
|-----------------------|----------------------------------------------------------------|
| Alarms                | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>    |
| Details               | <a href="#">Viewing Details, page 8-12</a>                     |
| Errors                | <a href="#">Viewing Shorthaul Errors, page 8-115</a>           |
| Notes                 | <a href="#">Viewing Notes, page 6-39</a>                       |
| Recent Events         | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>    |
| Shorthaul Performance | <a href="#">Viewing Shorthaul Performance Data, page 8-108</a> |
| Shorthaul Errors      | <a href="#">Viewing Shorthaul Errors, page 8-115</a>           |
| Status Contributors   | <a href="#">Viewing Status Contributors, page 8-10</a>         |
| Troubleshooting       | <a href="#">Viewing Troubleshooting, page 8-43</a>             |



## Note

To view all interfaces in your system, see [Interfaces Table, page 6-21](#).

# Card Tabs

Clicking on a card in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                                    |
|---------------------|--------------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>        |
| Details             | <a href="#">Viewing Details, page 8-12</a>                         |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                           |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>        |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>             |
| <b>Note</b>         | Only available when the card has child objects such as interfaces. |



## Note

To view all cards in your system, see [Cards Table, page 6-23](#).



# RAN Backhaul Tabs

Clicking on a RAN backhaul in a MWTM view may provide you with these tabs:

| Tab                  | Related Content                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alarms               | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>                                                                                                                                                             |
| Backhaul Errors      | <a href="#">Viewing Backhaul Errors, page 8-120</a> (Real-time data on the MWTM client)<br><a href="#">Displaying Backhaul Error Statistics, page 11-42</a> (Historical data on the MWTM web interface)                 |
| Backhaul Performance | <a href="#">Viewing Backhaul Performance Data, page 8-111</a> (Real-time data on the MWTM client)<br><a href="#">Displaying Backhaul Performance Statistics, page 11-36</a> (Historical data on the MWTM web interface) |
| Details              | <a href="#">Viewing Details, page 8-12</a>                                                                                                                                                                              |
| Notes                | <a href="#">Viewing Notes, page 6-39</a>                                                                                                                                                                                |
| RAN Shorthauls       | <a href="#">Viewing RAN Shorthauls, page 8-140</a>                                                                                                                                                                      |
| Recent Events        | <a href="#">Viewing Alarms and Recent Events, page 8-45</a>                                                                                                                                                             |
| Status Contributors  | <a href="#">Viewing Status Contributors, page 8-10</a>                                                                                                                                                                  |
| Troubleshooting      | <a href="#">Viewing Troubleshooting, page 8-43</a>                                                                                                                                                                      |



**Note**

To view all RAN backhails in your system, see [RAN Backhails Table, page 6-25](#).

## Physical and Management Interface Folder Tabs

The Physical folder that contains a list of the physical interfaces and cards that belong to the node. The Management Interface folder contains a list of interfaces that the MWTM uses to manage the node.

Clicking on a Physical or Management Interface folder in a MWTM view may provide you with these tabs:

| Tab                 | Related Content                                             |
|---------------------|-------------------------------------------------------------|
| Alarms              | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Details             | <a href="#">Viewing Details, page 8-12</a>                  |
| Notes               | <a href="#">Viewing Notes, page 6-39</a>                    |
| Recent Events       | <a href="#">Viewing Alarms and Recent Events, page 8-45</a> |
| Status Contributors | <a href="#">Viewing Status Contributors, page 8-10</a>      |





# APPENDIX **B**

## Command Reference

---

This appendix provides the format and a brief description of these Cisco Mobile Wireless Transport Manager (MWTM) commands, listed alphabetically. Each command is available on the:

- Server only (including Solaris and Linux).
- Server and Solaris or Linux clients only.
- Server and all clients (including windows) as indicated.

You can run commands from:

- *install\_directory/bin*  
where *install\_directory* is the directory where the MWTM server is installed (by default, */opt/CSCOsgm*).
- Alternatively, if you have the *install\_directory/bin* in your path, you can simply run commands from in your path.

This appendix contains:

- [General Commands, page B-1](#)
- [ITP-Only Commands, page B-85](#)
- [RAN-O-Only Commands, page B-130](#)



**Note**

---

General commands are for ITP and RAN-O networks; ITP commands are only for ITP networks.

---

## General Commands

General commands for the MWTM include:

- [mwtm, page B-5](#)
- [mwtm addcreds, page B-6](#)
- [mwtm addsnmpcomm, page B-6](#)
- [mwtm adduser, page B-7](#)
- [mwtm archivedirsize, page B-8](#)
- [mwtm authtype, page B-8](#)
- [mwtm backup, page B-9](#)

- [mwtm backupdir](#), page B-10
- [mwtm badloginalarm](#), page B-11
- [mwtm badlogindisable](#), page B-11
- [mwtm browserpath](#), page B-12
- [mwtm certgui](#), page B-12
- [mwtm certtool](#), page B-12
- [mwtm changes](#), page B-13
- [mwtm checksystem](#), page B-13
- [mwtm clean](#), page B-14
- [mwtm cleanall](#), page B-14
- [mwtm cleandb](#), page B-15
- [mwtm cleandiscover](#), page B-16
- [mwtm cliconntimer](#), page B-16
- [mwtm client](#), page B-17
- [mwtm clientfailoverprompt](#), page B-17
- [mwtm clientlogs](#), page B-18
- [mwtm clitimeout](#), page B-18
- [mwtm cmdlog](#), page B-18
- [mwtm collectstats](#), page B-19
- [mwtm console](#), page B-20
- [mwtm consolelogsize](#), page B-20
- [mwtm countnodes](#), page B-20
- [mwtm countobjects](#), page B-21
- [mwtm cwsetup](#), page B-21
- [mwtm datadir](#), page B-22
- [mwtm dbtool](#), page B-23
- [mwtm delete](#), page B-23
- [mwtm deletecreds](#), page B-24
- [mwtm deletesnmpcomm](#), page B-24
- [mwtm deluser](#), page B-25
- [mwtm disablepass](#), page B-25
- [mwtm disableuser](#), page B-26
- [mwtm discover](#), page B-26
- [mwtm diskmonitor](#), page B-26
- [mwtm enableuser](#), page B-27
- [mwtm eventautolog](#), page B-27
- [mwtm eventconfig](#), page B-28
- [mwtm eventeditor](#), page B-28

- [mwtm eventtool](#), page B-29
- [mwtm evilstop](#), page B-30
- [mwtm export](#), page B-30
- [mwtm export cw](#), page B-31
- [mwtm help](#), page B-32
- [mwtm importcw](#), page B-32
- [mwtm inactiveuserdays](#), page B-32
- [mwtm installlog](#), page B-33
- [mwtm inventorytool](#), page B-34
- [mwtm iosreport](#), page B-35
- [mwtm ipaccess](#), page B-35
- [mwtm jspport](#), page B-36
- [mwtm keytool](#), page B-36
- [mwtm killclients](#), page B-37
- [mwtm listusers](#), page B-37
- [mwtm logger](#), page B-38
- [mwtm logincreds](#), page B-38
- [mwtm logtimemode](#), page B-40
- [mwtm manage](#), page B-40
- [mwtm maxascirows](#), page B-42
- [mwtm maxevhist](#), page B-42
- [mwtm maxhtmlrows](#), page B-43
- [mwtm mldebug](#), page B-43
- [mwtm modifiesnmpcomm](#), page B-44
- [mwtm motd](#), page B-44
- [mwtm msglog](#), page B-45
- [mwtm msglogage](#), page B-45
- [mwtm msglogdir](#), page B-46
- [mwtm logsize](#), page B-39
- [mwtm netlog](#), page B-46
- [mwtm netlogger](#), page B-47
- [mwtm newlevel](#), page B-47
- [mwtm osinfo](#), page B-47
- [mwtm passwordage](#), page B-47
- [mwtm patchlog](#), page B-48
- [mwtm poll](#), page B-49
- [mwtm pollertimeout](#), page B-49
- [mwtm print](#), page B-49

- [mwtm props](#), page B-50
- [mwtm provisiontool](#), page B-50
- [mwtm purgedb](#), page B-51
- [mwtm readme](#), page B-52
- [mwtm reboot](#), page B-52
- [mwtm repdailyage](#), page B-52
- [mwtm rephelp](#), page B-53
- [mwtm rephourlyage](#), page B-53
- [mwtm restart](#), page B-53
- [mwtm restore](#), page B-54
- [mwtm restoreprops](#), page B-55
- [mwtm rootvars](#), page B-55
- [mwtm sechelp](#), page B-55
- [mwtm seclog](#), page B-55
- [mwtm secondaryserver](#), page B-56
- [mwtm servername](#), page B-57
- [mwtm setpath](#), page B-57
- [mwtm showcreds](#), page B-59
- [mwtm showsnmpcomm](#), page B-59
- [mwtm snmpcomm](#), page B-59
- [mwtm snmpconf](#), page B-60
- [mwtm snmpget](#), page B-60
- [mwtm snmphelp](#), page B-63
- [mwtm snmpmaxrows](#), page B-63
- [mwtm snmpnext](#), page B-63
- [mwtm snmpsetup](#), page B-65
- [mwtm snmpwalk](#), page B-66
- [mwtm sounddir](#), page B-69
- [mwtm ssl](#), page B-70
- [mwtm sslstatus](#), page B-71
- [mwtm start](#), page B-71
- [mwtm start client](#), page B-71
- [mwtm start jsp](#), page B-72
- [mwtm start pm](#), page B-72
- [mwtm start web](#), page B-72
- [mwtm status](#), page B-72
- [mwtm stop](#), page B-72
- [mwtm stopclients](#), page B-73

- [mwtm stop jsp, page B-73](#)
- [mwtm stop pm, page B-73](#)
- [mwtm stop web, page B-73](#)
- [mwtm superuser, page B-73](#)
- [mwtm syncusers, page B-74](#)
- [mwtm tac, page B-74](#)
- [mwtm termproxy, page B-75](#)
- [mwtm trapaccess, page B-75](#)
- [mwtm trapratelimit count, page B-76](#)
- [mwtm trapratelimit interval, page B-76](#)
- [mwtm trapsetup, page B-76](#)
- [mwtm trapstatus, page B-77](#)
- [mwtm tshootlog, page B-77](#)
- [mwtm uninstall, page B-78](#)
- [mwtm unknownage, page B-78](#)
- [mwtm updateuser, page B-78](#)
- [mwtm useraccess, page B-79](#)
- [mwtm userpass, page B-79](#)
- [mwtm version, page B-80](#)
- [mwtm viewlog, page B-80](#)
- [mwtm wall, page B-80](#)
- [mwtm webaccesslog, page B-81](#)
- [mwtm weberrorlog, page B-81](#)
- [mwtm weblogupdate, page B-82](#)
- [mwtm webnames, page B-83](#)
- [mwtm webport, page B-83](#)
- [mwtm webutil, page B-84](#)
- [mwtm who, page B-84](#)
- [mwtm xtermpath, page B-84](#)

## mwtm

### Server and Solaris or Linux Clients Only

#### Command Description

Displays the command syntax for the **mwtm** command and all of its options. The function of this command is identical to **mwtm help**.

MWTM help is network specific, so only the commands pertaining to each network type appear. If you set all network types, you can see all the commands.

**Related Topic**

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm addcreds

**Server Only****Full Syntax**

**mwtm addcreds** [-d *nodetype*] [-u *username* -n *enable username*] [-i *ipaddress*] [-r *protocoltype*]

**Command Description**

Adds credentials for a given IP address, if specified. Otherwise, credentials are added to the system as Default, which applies the specified credentials to all nodes in the MWTM database.

- To add credentials for a specific node type, specify **-d** and the **nodetype**, which can be:
  - **itp**—ITP nodes
  - **ons**—ONS nodes
  - **csr**—Cell Site Router (CSR) nodes (Cisco MWR and Cisco 3825)
  - **ran\_svc**—RAN\_SVC nodes
- To add username credentials, specify **-u** and the username.
- To add **enable** username credentials, specify **-n** and the **enable** username.
- To add credentials for a particular IP address only, specify **-i** and the IP address of the node.
- To add the protocol type, specify **-r** and one protocol, which can be:
  - **telnet**—Telnet access
  - **ssh**—Secure shell access

You must log in as the root user or superuser to use this command.

**Related Topic**

[Configuring Login Credentials, page 3-20](#)

## mwtm addsnmpcomm

**Full Syntax**

**mwtm addsnmpcomm** -i *ipaddress* [-r *retry* | -t *timeout* | -p *poll*] -c *community*

**Command Description**

Adds an SNMP configuration to the MWTM server.

- **-i ipaddress**—the IP address of the device (required)
- **-r retry**—the number of times to retry connecting to the device (optional)
- **-t timeout**—the timeout value, in seconds (optional)
- **-p poll**—the poll interval, in minutes (optional)
- **-c community**—the read community string of the device (required)



You do not need to restart the MWTM server.

**Related Topic**

- [mwtm deletesnmpcomm](#), page B-24
- [mwtm modifiesnmpcomm](#), page B-44
- [mwtm showsnmpcomm](#), page B-59
- [mwtm snmpsetup](#), page B-65

## mwtm adduser

**Server Only****Full Syntax**

**mwtm adduser** *[username]*

**Command Description**

If you enable MWTM User-Based Access, adds the specified user to the authentication list.

When you add a user, the MWTM prompts you for this information:

- User's password. When setting the password, follow the rules and considerations in [Creating Secure Passwords](#), page 2-7.
- Whether to force the user to change the password at the next log in. The default is not to force the user to change the password.
- Authentication level for the user. Valid levels are:
  - 1—Basic User
  - 2—Power User
  - 3—Network Operator
  - 4—Network Administrator
  - 5—System Administrator

You must log in as the root user or superuser to use this command.

**Note**

If you enable Solaris authentication, you must log in as the root user, not as superuser, to use this command (see [Implementing Secure User Access \(Server Only\)](#), page 2-2).

**Related Topic**

- [Configuring User Access](#), page 2-1
- [Implementing Secure User Access \(Server Only\)](#), page 2-2

## mwtm archivedirsize

### Server Only

#### Full Syntax

**mwtm archivedirsize** [*megs*]

#### Command Description

Sets the maximum size (in megabytes) of the console log archive directory.

To view help for this command, include the following parameter: -h.

## mwtm authtype

### Server Only

#### Full Syntax

**mwtm authtype** [**local** | **solaris** | **linux**]

#### Command Description

Configures MWTM security authentication:

- **local**—Allows creation of user accounts and passwords that are local to the MWTM system. When using this method, you manage user names, passwords, and access levels by using MWTM commands.
- **solaris**—Uses standard Solaris-based user accounts and passwords, as the */etc/nsswitch.conf* file specifies. You can provide authentication with the local */etc/passwd* file; from a distributed Network Information Services (NIS) system; or with any other authentication tool, such as RADIUS or TACACS+ (for details, see [Additional Authentication Tools, page 2-3](#)).
- **linux**—Uses standard Linux-based user accounts and passwords, as the */etc/nsswitch.conf* file specifies. You can provide authentication with the local */etc/passwd* file; from a distributed NIS system; or with any other authentication tool, such as RADIUS or TACACS+ (for details, see [Additional Authentication Tools, page 2-3](#)).



#### Note

When using the **solaris** or **linux** options, if you have enabled user access, you must enable SSL (see [Implementing SSL Support in the MWTM, page 2-22](#) to ensure secure passwords between the MWTM client and server.)

You must log in as the root user to use this command.

#### Related Topic

- [Configuring User Access, page 2-1](#)
- [Implementing Secure User Access \(Server Only\), page 2-2](#)

## mwtm backup

### Server Only

#### Command Description



#### Note

Since backups can be large, ensure that your file system has enough space to handle them.

Backs up MWTM data files to the MWTM installation directory. The MWTM automatically backs up all data files nightly at 1:30 AM; but, you can use this command to back up the files at any other time. If you installed the MWTM in:

- The default directory, */opt*, then the locations of the backup files are */opt/mwtm61-client-backup.tar.Z* and */opt/mwtm61-server-backup.tar.Z*.
- A different directory, then the backup files reside in that directory.

To restore the MWTM data files from the previous night's backup, use the **mwtm restore** command. Do not try to extract the backup files manually.

You must log in as the root user (not as a superuser) to use this command.



#### Note

The MWTM performs a database integrity check during the backup. If the check fails, the previous backup is not overwritten. Instead, the MWTM creates a new failed file (for example: *mwtm61-server-backup-failed.tar.Z*).

#### Related Topic

- [Configuring a Backup MWTM Server, page 3-10](#)
- [mwtm backupdays, page B-9](#)
- [mwtm backupdir, page B-10](#)
- [mwtm restore, page B-54](#)

## mwtm backupdays

### Server Only

#### Full Syntax

**mwtm backupdays** [*days*]

#### Command Description

This command sets the number of days to save backup files on the MWTM server and client. The default value is 1 day, but you can configure the MWTM to save multiple days of backup files.

This command accepts values from 1 to 30 days. If you attempt to set a value outside of this range, the MWTM responds with this message:

Value out of range of 1-30.

The MWTM stores backup files in the backup directory (see [mwtm backupdir, page B-10](#)). The MWTM uses this file naming convention when there are multiple backup files:

```
mwtm<releasenum>-[server|client]-backup.tar.[date].Z
```

For example:

```
mwtm61-client-backup.tar.[date].Z
```

```
mwtm61-server-backup.tar.[date].Z
```

If the number of backup days is more than one, and you run the **mwtm restore** command, the MWTM will prompt you for a server or client backup file to restore from (because there would be more than one backup file to choose from). See [mwtm restore, page B-54](#).

Here is an example of setting the number of backup days to 5 days:

```
./mwtm backupdays
```

```
Current value is: 1
```

```
Enter number of days to save backup files <1-30>: [1] 5
```

```
Setting number of days to save backup files to 5 days.
```

In this example, the MWTM saves backup files for the last five days. The MWTM deletes backup files that are older than five days.



#### Note

If you notice multiple backups, ensure that there is enough free space in the backupdir file system (see [mwtm backupdir, page B-10](#)).

#### Related Topic

- [Backing Up or Restoring MWTM Files \(Server Only\), page 2-32](#)
- [mwtm backupdir, page B-10](#)
- [mwtm restore, page B-54](#)

## mwtm backupdir

### Server Only

#### Full Syntax

```
mwtm backupdir [directory]
```

#### Command Description



#### Note

You must stop the MWTM server before performing this command. You are prompted whether to continue.

You can change the directory in which the MWTM stores its nightly backup files. The default backup directory is the directory in which the MWTM is installed. If you installed the MWTM in:

- The default directory, */opt*, then the default backup directory is also */opt*.
- A different directory, then the default backup directory is that directory.

If you specify a new directory that does not exist, the MWTM does not change the directory and issues an appropriate message.

You must log in as the root user to use this command.

**Related Topic**

- [Configuring a Backup MWTM Server, page 3-10](#)
- [mwtm backupdays, page B-9](#)

## mwtm badloginalarm

**Server Only****Full Syntax**

**mwtm badloginalarm** [*number-of-attempts* | **clear**]

**Command Description**

If you enable MWTM User-Based Access, number of unsuccessful log-in attempts allowed before the MWTM generates an alarm.

The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 5 unsuccessful attempts.

The MWTM records alarms in the system security log file. The default path and filename for the system security log file is */opt/CSCOs/gm/logs/sgmSecurityLog.txt*. If you installed the MWTM in a directory other than */opt*, then the system security log file resides in that directory.

To view the system security log file, enter **mwtm seclog**. You can also view the system security log on the MWTM System Security Log web page (see [Displaying the Contents of the System Security Log \(Server Only\), page 2-18](#)).

To disable this function (that is, to prevent the MWTM from automatically generating an alarm after unsuccessful log-in attempts), enter **mwtm badloginalarm clear**.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Automatically Disabling Users and Passwords \(Server Only\), page 2-11](#)

## mwtm badlogindisable

**Server Only****Full Syntax**

**mwtm badlogindisable** [*number-of-attempts* | **clear**]

**Command Description**

If you enable MWTM User-Based Access, number of unsuccessful log-in attempts by a user allowed before the MWTM disables the user's authentication. The MWTM does not delete the user from the authentication list, the MWTM only disables the user's authentication. To re-enable the user's authentication, use the **mwtm enableuser** command.

The valid range is 1 unsuccessful attempt to an unlimited number of unsuccessful attempts. The default value is 10 unsuccessful attempts.

To disable this function (that is, to prevent the MWTM from automatically disabling a user's authentication after unsuccessful log-in attempts), enter **mwtm badlogindisable clear**.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Automatically Disabling Users and Passwords \(Server Only\), page 2-11](#)

## mwtm browserpath

**Server and Solaris or Linux Clients Only****Command Description**

Sets a user-defined MWTM web browser path and verifies that the browser specified by the user exists.

You must log in as the root user (not as a superuser) to use this command.

**Related Topic**

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm certgui

**Solaris Clients Only****Command Description**

If you enable the Secure Sockets Layer (SSL) on your MWTM system, opens the MWTM Certificate Tool window in which you manage SSL certificates on the MWTM client.

**Note**

If you installed the MWTM server and client on the same workstation, running this command is not necessary. Instead, when you use the **mwtm keytool** command to manage SSL certificates on the server, the MWTM automatically manages the certificates on the client.

You must log in as the root user (not as a superuser) to use this command in Solaris.

**Related Topic**

[Launching the MWTM Certificate Tool for SSL, page 2-26](#)

## mwtm certtool

**Server and Solaris Clients Only****Full Syntax**

```
mwtm certtool [clear | delete alias | export alias [-file filename] | import alias [-file filename] | list]
```

**Command Description**

If you enable the Secure Sockets Layer (SSL) on your MWTM system, you can use this command to manage SSL certificates on the MWTM client from the command line.

**Note**

If you installed the MWTM server and client on the same workstation, running this command is not necessary. Instead, when you use the **mwtm keytool** command to manage SSL certificates on the server, the MWTM automatically manages the certificates on the client.

Use these keywords and arguments with this command:

- **import alias [-file filename]**—Imports a signed SSL certificate in X.509 format. This is the most common use for this command.

The *alias* argument can be any character string; the hostname of the server from which you are importing the certificate is a good choice.

To import the certificate from a file, specify the optional **-file** keyword and a filename.

- **export alias [-file filename]**—Exports the specified SSL certificate in X.509 format.

To export the certificate to a file, specify the optional **-file** keyword and a filename.

- **list**—Lists all SSL certificates on the MWTM client.
- **delete alias**—Removes the specified SSL certificate from the MWTM client.
- **clear**—Removes all SSL certificates from the MWTM client.

**Solaris Only:** You must log in as the root user (not as a superuser) to use this command in Solaris.

**Related Topic**

[Importing an SSL Certificate to an MWTM Client, page 2-27](#)

## mwtm changes

**Server Only****Command Description**

Displays the contents of the MWTM CHANGES file. The CHANGES file lists all bugs that have been resolved in the MWTM, sorted by release. If you installed the MWTM in:

- The default directory, */opt*, then the MWTM CHANGES file resides in the */opt/CSCOs/gm/install* directory.
- A different directory, then the file resides in that directory.

## mwtm checksystem

**Server Only****Command Description**

Checks the system for a server installation and reviews the:

- System requirements
- TCP/IP address and port usage checks
- Disk space usage check
- Server summary

- Error summary

You must log in as the root user (not as a superuser) to use all features of this command. The *logs/troubleshooting* folder has limited permissions to read when the user is not a root user.

## mwtm clean

### Server Only

#### Command Description

Removes all MWTM data from the MWTM server, excluding message log files, backup files, and report files. This command restores the MWTM server to a state that would exist after a new installation of the MWTM; *except for the message log files, backup files, and report files.*

Removed data includes all:

- MWTM data
- Notes
- Preferences
- Security settings
- Route files
- GTT files
- Address table files
- Seed files
- Event filters
- Report control files
- Views
- Any user-created files stored in the MWTM directories

You must log in as the root user (not as a superuser) to use this command.

## mwtm cleanall

### Server Only

#### Command Description

Removes all MWTM data from the MWTM server, including message log files, backup files, report files, configuration settings, and security settings. This command restores the MWTM server to a state that would exist after a new installation of the MWTM.

Data removed includes all:

- MWTM data
- Notes
- Preferences
- Security settings
- Route files



- GTT files
- Address table files
- Seed files
- Event filters
- Report control files
- Views
- Any user-created files stored in the MWTM directories

You must log in as the root user (not as a superuser) to use this command.

## mwtm cleandb

### Server Only

#### Command Description

Removes all MWTM data from the MWTM server, including the:

- Core data model database
- All view files
- Notes associated with objects
- Event filters
- MWTM data
- Any user-created files stored in the MWTM directories

This command restores the MWTM server to a state that would exist after a new installation of the MWTM; *except for the presence of the retained files.*

The following data is excluded:

- Message log files
- Backup files
- Report files
- Configuration settings
- Security settings
- User credentials
- Route files
- GTT files
- Address table files

You must log in as the root user (not as a superuser) to use this command.

## mwtm cleandiscover

### Server Only

### Full Syntax

**mwtm cleandiscover** [*seed-node*] [*seed-node*]...

### Command Description

You can use this command to delete all current network data and begin a clean discovery of the network from the command line. Use the *seed-node* arguments to specify the DNS names or IP addresses of one or more seed nodes.



### Note

When you begin a clean discovery, the MWTM stops any real-time polls that are running and issues appropriate messages.

Running this command does not remove any notes, preferences, route files, views, message log files, backup files, or report files, nor any user-created files stored in the MWTM directories.

You must log in as the root user or superuser to use this command.

### Related Topic

[Discovering Your Network, page 4-4](#)

## mwtm cliconntimer

### Server Only

### Full Syntax

**mwtm cliconntimer** [*number-of-seconds* | **clear**]

### Command Description

Specifies how long, in seconds, an MWTM client should wait for a message from the MWTM server before the client attempts to contact the server and takes one of these actions. If the server:

- Responds to the client, the client reconnects to the server.
- Does not respond to the client, but a backup server is configured, the client attempts to connect to the backup server.
- Does not respond to the client and no backup server is configured, the client displays a dialog box with this message:

```
Connection to the server has timed out.
Client could not establish 2-way communications with the server.
If you are running through a VPN you may have entered the wrong client IP address.
```

Click **OK** to exit the client.

The MWTM writes this message to the client console log:

- Solaris client—*/opt/CSCOsgmClient/logs/sgmConsoleLog.txt*
- Windows client—*C:\Program Files\Cisco Systems\MWTM Client\logs\consoleLog.txt*

The valid range is 10 seconds to an unlimited number of seconds. The default value is 60 seconds.

To restore the default timeout of 60 seconds, enter the **mwtm cliconnntimer clear** command.

Any changes you make take effect when you restart the MWTM server.

You must log in as the root user or superuser to use this command.

## mwtm client

### Solaris or Linux Clients Only

#### Full Syntax

**mwtm client** [*hostname*]

#### Command Description

Starts an MWTM client on the specified host. If no hostname is specified, starts an MWTM client on the default host, as specified during installation. See [Connecting to a New Server, page 5-43](#) for information about determining the default host.

If you access a remote workstation by Telnet, the DISPLAY variable must be set to your local display or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually. See [Setting the DISPLAY Variable for Solaris or Linux Clients, page 4-3](#) for details.

#### Related Topic

[Starting the MWTM Client, page 4-2](#)

## mwtm clientfailoverprompt

### Solaris or Linux Clients Only

#### Full Syntax

**mwtm clientfailoverprompt** [**enable** | **disable** | **status**]

#### Command Description

Indicates whether or not a prompt is issued when the primary server fails over to the secondary server:

- **enable**—Enables the prompt, and you are prompted to provide credentials before failing over to the secondary server.



#### Note

MWTM user access must be enabled, and your user ID and password must be the same on both servers. Also, ensure that the backup server is defined (see [Configuring a Backup MWTM Server, page 3-10](#)).

- **disable**—Disables the prompt, and you are connected to the secondary server automatically.
- **status**—Displays the current status of prompt (whether enabled or disabled).

You must log in as the root user or superuser to use this command.

## mwtm clientlogs

### Server Only

#### Command Description

Uses PAGER to display the MWTM client log files.

The MWTM client log files contain client console output for all MWTM clients, one file per local or remote client. The MWTM automatically creates the file for a client when the client starts. If you installed the MWTM in:

- The default directory, */opt*, then the MWTM client log file resides in the */opt/CSCOs/gm/logs/clientLogs* directory.
- A different directory, then the file resides in that directory.

## mwtm clitimeout

### Server Only

#### Full Syntax

**mwtm clitimeout** [*mins* | **clear**]

#### Command Description

Specifies how long, in minutes, an MWTM client can be inactive before the MWTM automatically disconnects it.

This function is disabled by default. If you do not specify this command, clients are never disconnected as a result of inactivity.

If you enter the **mwtm clitimeout** command, the valid range is 1 minute to an unlimited number of minutes. No default value exists.

If you enable this function and you want to disable it (that is, never disconnect a client as a result of inactivity), enter the **mwtm clitimeout clear** command.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Automatically Disabling Users and Passwords \(Server Only\), page 2-11](#)

## mwtm cmdlog

### Server Only

#### Full Syntax

**mwtm cmdlog** [**clear** | **-r**]

#### Command Description

Uses PAGER to display the contents of the system command log. The system command log lists:

- All **mwtm** commands that were entered for the MWTM server.

- The time each command was entered.
- The user who entered the command.

To clear the log, enter **mwtm cmdlog clear**.

To display the contents of the log in reverse order, with the most recent commands at the beginning of the log, enter **mwtm cmdlog -r**.

You must log in as the root user or superuser to use this command.

## mwtm collectstats

### Server Only

#### Full Syntax

**mwtm collectstats** [-h *hostname(s)*] {-d *date(s)* | -s *starttime* -e *endtime*} [**clean**]

#### Command Description

Gathers report and event information from the database for the input criteria. The output appears here:

*/opt/CSCOsrgm/tmp/cisco\_mwtm\_stats\_<date>\_<timestamp>.zip*

Use the following keywords and arguments with this command:

- **-h *hostname(s)***—Narrow your search to specific devices by entering each hostname individually. For example:  

```
./mwtm collectstats -h hostname1 hostname2 hostname3
```
- **-d *date(s)***—Collects reports and events for the devices indicated for the given specific dates. The date format must be in YYYYMMDD. Enter each date individually. For example:  

```
./mwtm collectstats -h hostname1 hostname2 hostname3 20070621 20070622 20070623
```
- **-s *starttime*** and **-e *endtime***—Collects reports and events for the devices indicated from a start time to an end time. The date format must be in YYYYMMDD-HHMM. For example:  

```
./mwtm collectstats -h hostname1 hostname2 hostname3 -s 02232008-1500 -e 03012008-2300
```
- **clean**—Removes older .zip files.

If no data is available, a message appears, and the MWTM does not create a .zip file.

If you specify hostnames, the MWTM creates a separate log file for each hostname with the events and trap details. For each report category, the MWTM creates a log file in .csv format, with a name similar to:

```
cisco_mwtm_stats_report_<NameOfReport>.csv
cisco_mwtm_stats_event_trap_<Hostname>.csv
```

In addition, the MWTM creates a consolidated log file for all events and all report data separately.

You must log in as the root user or superuser to use this command.

## mwtm confirmfailover

### Server, Web and Java Clients

#### Full Syntax

**mwtm confirmfailover** [*enable* | *disable* | *status*]

#### Command Description

Sets a system-wide server preference to enable or disable seamless automatic login using previously-authenticated credentials. When set to enable, clients automatically log in to the backup MWTM server in the case of a failover.

#### Reviewer: What does the status option do?

You must log in as the root user or superuser to use this command.

## mwtm console

### Server Only

#### Command Description

Displays the contents of the console log file, *sgmConsoleLog.latest*. The console log file contains unexpected error and warning messages from the MWTM server, such as those that might occur if the MWTM server cannot start.

You must log in as the root user or superuser to use this command.

## mwtm consolelogsize

### Server Only

#### Full Syntax

**mwtm consolelogsize** [*megs*]

#### Command Description

Sets the maximum size (in megabytes) of the console log file.

To view help for this command, include the following parameter: -h.

## mwtm countnodes

### Server Only

#### Command Description

Displays the number of nodes in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm countobjects

### Server Only

#### Command Description

Displays a count of all objects in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm cwsetup

### Solaris Server Only

#### Full Syntax

**mwtm cwsetup** [install | uninstall]

#### Command Description

Manages the integration of the MWTM with CiscoWorks:

- **install**—Checks to see which CiscoWorks files are installed and installs additional files as necessary. Use this command to integrate the MWTM and CiscoWorks in these instances:
  - You installed CiscoWorks after you installed the MWTM.
  - The MWTM and CiscoWorks are no longer integrated for some reason.
- **uninstall**—Removes MWTM files from the CiscoWorks area.



---

**Note** Always run **mwtm cwsetup uninstall** before uninstalling CiscoWorks from your system.

---

- The command prompts you to enter:
  - The CiscoWorks server name
  - The port number for the CiscoWorks web server (the default setting is 1741)
  - The secure port number for the CiscoWorks web server (the default setting is 443)
  - Whether or not CiscoWorks security is enabled



---

**Note** Changing CiscoWorks settings by using the **mwtm cwsetup** command sets all clients on the MWTM server to use these settings. You can configure a particular MWTM client to use different CiscoWorks settings by changing the client's preferences. See [Changing CiscoWorks Server Settings, page 5-13](#).

---

You must log in as the root user (not as a superuser) to use this command.

You must restart the MWTM server for your changes to take effect. After the server restart, you can launch these applications from the MWTM Tools menu:

- CiscoWorks Device Center
- CiscoView
- Content Services Gateway (CSG) Service Manager

- GPRS Gateway Support Node (GGSN) Service Manager

Also, you can launch the MWTM web interface from the CiscoWorks dashboard. In this scenario, CiscoWorks and MWTM are running on the same server.

**Note**

The MWTM attempts to launch the URL of the service manager that resides on the LMS server. If the service manager is not installed on the LMS server, you will receive an HTTP 404 error. To prevent this error, ensure that the service managers are installed on the LMS server, or remove the CSG or GGSN network setting with the [mwtm manage, page B-40](#) command.

**Related Topic**

[Changing CiscoWorks Server Settings, page 5-13](#)

## mwtm datadir

**Server Only****Full Syntax**

**mwtm datadir** [*directory*]

**Command Description****Note**

You must stop the MWTM server before performing this command. You are prompted whether to continue.

Sets the directory in which the MWTM stores data files. Use this command when you want to move the data directory to a larger filing system to accommodate the increasing size of the directory.

The default directory for data files resides in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the default directory is */opt/CSCOsgm/data*.
- A different directory, then the default directory resides in that directory.

Use this command if you want to store data files in a different directory; for example, in a Network File System location on another server.

**Note**

This command copies all files in the current directory to the new directory. If you are not logged in as the superuser and you do not own the new directory, you might not be able to copy the files. In that case, you must specify a directory that you own or log in as the root user.

Do not set the new directory to any of these: */usr*, */var*, */opt*, or */tmp*.

Do not set the new directory to the same directory in which you are storing GTT files (**mwtm gttmdir**), message log files (**mwtm msglogdir**), route table files (**mwtm routedir**), or address table files (**mwtm atbldir**).

After you change the directory, the MWTM asks if you want to restart the MWTM server. The new directory takes effect when you restart the MWTM server.



You must log in as the root user or superuser to use this command.

## mwtm dbtool

### Server Only

#### Full Syntax

**mwtm dbtool** {*SQL*}

#### Command Description

Issues a SQL query against the MWTM database. Use a standard SQL query, except replace any instances of the asterisk (\*) with a question mark (?). For example, a sample SQL query might be:

```
"select * from events"
```

Using the mwtm **dbtool** command, this SQL query would be:

```
mwtm dbtool "select ? from events"
```

You must log in as the root user or superuser to use this command.

## mwtm delete

### Server Only

#### Full Syntax

**mwtm delete** [**all** | **node** [**all** | *node* [*node*]...] | **sp** [**all** | *point-code:net* [*point-code:net*]...] | **linkset** [**all** | *node/linkset* [*node/linkset*]...]

#### Command Description

Deletes objects from the MWTM database.

- **all**—Deletes all objects from the MWTM database.
- **node all**—Deletes all nodes from the MWTM database.
- **node** *node* [*node*]...—Deletes one or more nodes from the MWTM database. Use the *node* arguments to specify one or more nodes.
- **sp all**—Deletes all nodes from the MWTM database.
- **sp** *point-code:net* [*point-code:net*]...—Deletes one or more signaling points from the MWTM database. Use the *point-code:net* arguments to specify one or more signaling points, which the point code and network name identify; for example, 1.22.0:net0.
- **linkset all**—Deletes all linksets from the MWTM database.
- **linkset** *node/linkset* [*node/linkset*]...—Deletes one or more linksets from the MWTM database. Use the *node/linkset* arguments to specify one or more linksets associated with specific nodes.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Deleting Objects, page 6-40](#)

## mwtm deletecreds

### Server Only

#### Full Syntax

**mwtm deletecreds** [-d *nodetype*] [-i *ipaddress*] [-a]

#### Command Description

Deletes credentials for a given IP address, if specified. Otherwise, Default credentials are deleted. To delete:

- Credentials for a specific node type, specify **-d** and the nodetype:
  - **itp**—ITP nodes
  - **ons**—ONS nodes
  - **csr**—Cell Site Router (CSR) nodes
  - **ran\_svc**—RAN\_SVC nodes
- Credentials for a particular IP address only, specify **-i** and the IP address of the node.
- All credentials, specify **-a**.

#### Related Topic

[Configuring Login Credentials, page 3-20](#)

## mwtm deletesnmpcomm

#### Full Syntax

**mwtm deletesnmpcomm** -i *ipaddress*

#### Command Description

Deletes an SNMP configuration from the MWTM server.

**-i *ipaddress***—the IP address of the device (required)

You do not need to restart the MWTM server.

#### Related Topic

- [mwtm addsnmpcomm, page B-6](#)
- [mwtm modifiesnmpcomm, page B-44](#)
- [mwtm showsnmpcomm, page B-59](#)
- [mwtm snmpsetup, page B-65](#)

## mwtm deluser

### Server Only

#### Full Syntax

**mwtm deluser** *[username]*

#### Command Description

If you enable MWTM user-based access, deletes the specified user from the authentication list. To add the user back to the list, use the **mwtm adduser** command.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Manually Disabling Users and Passwords \(Server Only\), page 2-13](#)

## mwtm disablepass

### Server Only

#### Full Syntax

**mwtm disablepass** *[username]*

#### Command Description

If you enable the MWTM User-Based Access, and set **mwtm authtype** to **local**, disables the specified user's authentication and password. The MWTM does not delete the user from the authentication list; rather, the MWTM only disables the user's authentication and password. To re-enable the user's authentication with:

- The same password as before, use the **mwtm enableuser** command.
- A new password, use the **mwtm userpass** command.



#### Note

The user can re-enable authentication with a new password by attempting to log in by using the old password; the MWTM then prompts the user for a new password.

If you set **mwtm authtype** to **solaris** or **linux**, you cannot use this command; instead, you must manage passwords on the external authentication servers.

You must log in as the root user or superuser to use this command. You must also set the **mwtm authtype** to **local**.

#### Related Topic

[Manually Disabling Users and Passwords \(Server Only\), page 2-13](#)

## mwtm disableuser

### Server Only

#### Full Syntax

**mwtm disableuser** [*username*]

#### Command Description

If you enable MWTM User-Based Access, disables the specified user's authentication. The MWTM does not delete the user from the authentication list, the MWTM only disables the user's authentication. To re-enable the user's authentication with:

- The same password as before, use the **mwtm enableuser** command.
- A new password, use the **mwtm userpass** command.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Manually Disabling Users and Passwords \(Server Only\), page 2-13](#)

## mwtm discover

### Server Only

#### Full Syntax

**mwtm discover** [*seed-node*] [*seed-node*]...

#### Command Description

You use this command to discover the network from the command line. Use the *seed-node* arguments to specify the DNS names or IP addresses of one or more seed nodes.



#### Note

---

This command does not perform a clean discovery. To do so, see the **mwtm cleandiscover** command.

---

You must log in as the root user or superuser to use this command.

#### Related Topic

[Discovering Your Network, page 4-4](#)

## mwtm diskmonitor

### Server Only

#### Full Syntax

**mwtm diskmonitor** [*enable* | *disable* | *status*] | **warning** *megs* | **shutdown** *megs*

### Command Description

Monitors the disk space usage of the MWTM installed directories. When enabled, a script (*diskWatcher.sh*) runs every hour to check two thresholds:

- **Warning**—Warns the MWTM operator when the disk space usage exceeds the threshold value. The MWTM logs the warning in the *sgmConsoleLog.txt* file. For example:

```
WARNING: The following partition is getting low on free disk space:
/opt
Space left = 905 MB
```

- **Shutdown**—Shuts down the MWTM server when the disk space usage exceeds the threshold value.

The parameters of the **mwtm diskmonitor** command are:

- **enable**—Enables the hourly check of disk space usage of MWTM installed directories.
- **disable**—Disables the hourly check of disk space usage of MWTM installed directories.
- **status**—Displays the current status of the disk monitor feature (whether enabled or disabled).
- **warning megs**—Sets the warning threshold in MBs. The default setting is 1000 MB.
- **shutdown megs**—Sets the shutdown threshold in MBs. The default setting is 100 MB.

You must log in as the root user or superuser to use this command.

## mwtm enableuser

### Server Only

### Full Syntax

**mwtm enableuser** [*username*]

### Command Description

If you enable MWTM user-based access, re-enables the specified user's authentication, which had been disabled either automatically by the MWTM or by a superuser.

The user's authentication is re-enabled with the same password as before.

You must log in as the root user or superuser to use this command.

### Related Topic

[Enabling and Changing Users and Passwords \(Server Only\), page 2-14](#)

## mwtm eventautolog

### Server Only

### Full Syntax

**mwtm eventautolog** [*clear* | *-r*]

### Command Description

Uses PAGER to display the contents of the MWTM event automation log. The event automation log lists all messages generated by scripts launched by event automation.

To clear the log and restart the server, enter **mwtm eventautolog clear**.

To display the contents of the log in reverse order, with the most recent events at the beginning of the log, enter **mwtm eventautolog -r**.

You must log in as the root user or superuser to use this command.

## mwtm eventconfig

### Server Only

#### Full Syntax

**mwtm eventconfig** [**view** | **edit** | **restore** | **master**]

#### Command Description

Allows you to manage the event configuration:

- To view the event configuration file, use the **mwtm eventconfig view** command.
- To edit the event configuration file in your environment with a text editor, use the **mwtm eventconfig edit** command. (The default text editor is 'vi'.)
- To restore the event configuration file to the last active copy, use the **mwtm eventconfig restore** command.
- To restore the event configuration file to the master copy (the default copy shipped with the MWTM), use the **mwtm eventconfig master** command.

You must log in as the root user or superuser to use this command.

## mwtm eventeditor

### Solaris or Linux Clients Only

#### Full Syntax

**mwtm eventeditor** [*hostname*]

#### Command Description

Starts an MWTM Event Editor on the specified host. If no hostname is specified, starts an MWTM Event Editor on the default host, as specified during installation. See [Connecting to a New Server, page 5-43](#) for information about determining the default host.

For more information about the MWTM Event Editor, see [Changing the Way the MWTM Processes Events, page 9-35](#).

If you Telnet into a remote workstation, the DISPLAY variable must be set to your local display, or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually (see [Setting the DISPLAY Variable for Solaris or Linux Clients, page 4-3](#)).

#### Related Topic

- [Chapter 9, “Managing Alarms and Events”](#)

## mwtm eventtool

### Server Only

### Full Syntax

**mwtm eventtool** {-a *actionName*} {*parameters*}

### Command Description

Invokes MWTM event API operations.

These action names (and any corresponding required parameters) can be specified with the -a option:

| Option | Action Names             | Required Parameters        |
|--------|--------------------------|----------------------------|
| -a     | acknowledgeEvents        | -l or -L<br>-u<br>-n       |
|        | appendNote               | -e<br>-n<br>-u             |
|        | changeSeverities         | -s<br>-l or -L<br>-u<br>-n |
|        | clearEvents              | -l or -L<br>-u<br>-n       |
|        | deleteEvents             | -l or -L<br>-u<br>-n       |
|        | getAllEventsAsTraps      | -t                         |
|        | getFilteredEventsAsTraps | -t<br>-f                   |
|        | getNote                  | -e                         |
|        | setNote                  | -e<br>-n<br>-u             |

These parameters can be used:

| Parameter | Description                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| -e        | Specifies an event ID parameter.                                                                                                                     |
| -f        | Specifies a file name for EventFilter, which is an XML element defined in MWTM WSDL definitions.                                                     |
| -l        | Specifies a file name for EventIDList, which is an XML element defined in MWTM WSDL definitions.                                                     |
| -n        | Specifies an event note string.                                                                                                                      |
| -s        | Specifies an event severity.                                                                                                                         |
| -t        | Specifies a file name for TrapTarget, which is an XML element defined in MWTM WSDL definitions.                                                      |
| -u        | Specifies a user ID for event operation.                                                                                                             |
| -H        | Specifies a hostname to connect to. If unspecified, the default value is obtained from the MWTM server System.properties file, SERVER_NAME property. |
| -p        | Specifies a port to connect to. If unspecified, the default value is obtained from the MWTM server System.properties file, WEB_PORT property.        |
| -L        | Specifies a list of event IDs, separated by ' '.                                                                                                     |
| -S        | Specifies whether to use SSL (https) for NBAPI access. Default is no SSL.                                                                            |
| -h        | Prints help information.                                                                                                                             |

You must log in as the root user or superuser to use this command.

#### Related Documentation

See the *Cisco Mobile Wireless Transport Manager 6.1 OSS Integration Guide*.

## mwtm evilstop

### Server Only

#### Command Description

Forcefully stops all MWTM servers on the local host. This command can be useful if a normal **mwtm stop** does not stop the servers.

You must log in as the root user (not as a superuser) to use this command.

## mwtm export

### Server Only

#### Full Syntax

**mwtm export** [-d {bar | comma | tab}] [all | as | asp | aspa | links | linksets | nodes | mwtmp | sps]



**Command Description**

Exports current MWTM data.

By default, the MWTM separates data fields with vertical bars (|). However, you can specify commas (,) or tabs as the separator:

- **-d bar**—Separate data fields with vertical bars (|). This is the default setting.
- **-d comma**—Separate data fields with commas (,).
- **-d tab**—Separate data fields with tabs.

By default, the MWTM exports all data. However, you can limit the data that the MWTM exports:

- **all**—Exports all current MWTM data. This is the default selection.
- **as**—Exports application server data only.
- **asp**—Exports application server process data only.
- **aspa**—Exports application server process association data only.
- **links**—Exports link data only.
- **linksets**—Exports linkset data only.



**Note** Links and linkset output totals might not match what appears in the MWTM client (see [ITP Specific FAQs, page C-13](#)).

- **nodes**—Exports node data only.
- **mwtm**—Exports signaling gateway-mated pair data only.
- **sps**—Exports signaling point data only.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Exporting Data, page 5-38](#)

## mwtm export cw

**Solaris Server Only****Full Syntax**

**mwtm export cw**

**Command Description**

Exports current MWTM node names, and read and write SNMP community names, in CiscoWorks import format, with fields separated by commas (,). You can export this data to a file, then use the file to import the nodes into the CiscoWorks database.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Exporting Data, page 5-38](#).

## mwtm help

### Server and Solaris or Linux Clients Only

#### Full Syntax

**mwtm help** [*keyword*]

#### Command Description

Displays the command syntax for the **mwtm** command and all of its options. The function of this command is identical to **mwtm**.

MWTM help is network specific, so only the commands pertaining to each network type appear. If you set all network types, you can see all the commands.

To see the syntax for a specific command, enter **mwtm help** and that command. For example, if you enter **mwtm help restart**, the MWTM displays:

```
mwtm restart - Restarts all MWTM Servers on the local host.
mwtm restart web - Restarts Web servers on the local host.
mwtm restart jsp - Restarts JSP servers on the local host.
mwtm restart pm - Restarts Process Manager on the local host.
```

#### Related Topic

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm importcw

#### Full Syntax

**mwtm importcw** [*cwfile*]

#### Command Description

Imports node hostname and read-community strings from the CiscoWorks server to MWTM.

*cwfile*—File name of the CiscoWorks export file (export format must be in CSV file format).

You must log in as the root user or superuser to use this command. You do not need to restart the server to activate this command. After running this command, the MWTM discovers the imported nodes.

## mwtm inactiveuserdays

### Server Only

#### Full Syntax

**mwtm inactiveuserdays** [*number-of-days* | **clear**]

#### Command Description

If you enable MWTM user-based access, number of days a user can be inactive before disabling that user account.

This function is disabled by default. If you do not specify this command, user accounts are never disabled as a result of inactivity.

If you enter the **mwtm inactiveuserdays** command, the valid range is 1 day to an unlimited number of days. There is no default setting.

If you have enabled this function and you want to disable it (that is, prevent the MWTM from automatically disabling user accounts as a result of inactivity), enter **mwtm inactiveuserdays clear**.

To re-enable the user's authentication, use the **mwtm enableuser** command.

You must log in as the root user or superuser to use this command.

#### Related Topics

- [Chapter 2, “Configuring Security”](#)
- [Automatically Disabling Users and Passwords \(Server Only\), page 2-11](#)

## mwtm installlog

### Server and Solaris or Linux Clients Only

#### Full Syntax

**mwtm installlog** [server | client]

#### Command Description

Displays the latest install log for the **server** or **client**. If you do not specify **server** or **client**, displays the latest install log for both the server and client.

You must log in as the root user or superuser to use this command.

# mwtm inventorytool

## Server Only

### Full Syntax

**mwtm inventorytool -a** *actionName* [*parameters*]

### Command Description

Invokes inventory API operations.

These action names (and any corresponding required parameters) can be specified with the **-a** option:

| Option | Action Names     | Parameters |
|--------|------------------|------------|
| -a     | getAllINEs       | -c         |
|        | getRootNEs       | -H         |
|        |                  | -p         |
|        |                  | -S         |
|        |                  | -h         |
|        | getNE            | -f         |
|        | getChildNEs      | -c         |
|        | getDescendantNEs | -H         |
|        | getNote          | -p         |
|        |                  | -S         |
|        |                  | -h         |
|        | setNote          | -f         |
|        | appendNote       | -u         |
|        |                  | -n         |
|        |                  | -H         |
|        |                  | -p         |
|        |                  | -S         |
|        |                  | -h         |

You can use these parameters:

| Parameter | Description                                                                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -c        | (Optional) Specifies the context of the inventory. Valid contexts include: <b>config</b> , <b>monitor</b> , and <b>all</b> . If unspecified, the default value is <b>all</b> . |
| -f        | Specifies a fully qualified domain name (FQDN).                                                                                                                                |
| -S        | (Optional) Specifies whether to use SSL (https) for NBAPI access. The default is no SSL.                                                                                       |
| -n        | Specifies a note string. Enclose the string in double quotes.                                                                                                                  |

| Parameter | Description                                                                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -u        | Specifies a user ID for inventory operation.                                                                                                                                               |
| -H        | (Optional) Specifies a hostname to connect to. If unspecified, the system obtains the default value from the MWTM server <i>System.properties</i> file, <code>SERVER_NAME</code> property. |
| -p        | (Optional) Specifies a port to which to connect. If unspecified, the system obtains the default value from the MWTM server <i>System.properties</i> file, <code>WEB_PORT</code> property.  |
| -h        | (Optional) Prints help information.                                                                                                                                                        |

You must log in as the root user or superuser to use this command.

#### Related Documentation

See the *Cisco Mobile Wireless Transport Manager 6.1 OSS Integration Guide*.

## mwtm iosreport

#### Server Only

#### Full Syntax

**mwtm iosreport**

#### Command Description

You use this command to create a report, in CSV format, of the IOS versions of all the nodes that the MWTM is managing. The format for the output is:

*node name, custom name, node type, IOS version, serial number*

For example:

```
./mwtm iosreport
'NODE NAME','Custom Name','NODE TYPE','IOS VERSION','SERIAL NUMBER',
'ems15454ec.cisco.com',null,'CiscoONS15454','7.2','SMA08040634',
'ems1900ke.cisco.com',null,'CiscoMWR-1900','12.4(20070313:074027)','JMX0650L264',
```

You must log in as the root user or superuser to use this command.

## mwtm ipaccess

#### Server Only

#### Full Syntax

**mwtm ipaccess** [**add** [*ip-addr*] | **clear** | **edit** | **list** | **rem** [*ip-addr*] | **sample**]

#### Command Description

You use this command to create and manage a list of client IP addresses that can connect to the MWTM server.

The list of allowed client IP addresses resides in the *ipaccess.conf* file. By default, when you first install the MWTM, the *ipaccess.conf* file does not exist and all client IP addresses can connect to the MWTM server. To create the *ipaccess.conf* file and specify the list of allowed client IP addresses, use one of these keywords:

- **add**—Add the specified client IP address to the *ipaccess.conf* file. If the *ipaccess.conf* file does not already exist, this command creates a file with the first entry.
- **clear**—Remove all client IP addresses from the *ipaccess.conf* file and allow connections from any MWTM client IP address.
- **edit**—Open and edit the *ipaccess.conf* file directly. If the *ipaccess.conf* file does not already exist, this command creates an empty file.
- **list**—List all client IP addresses currently in the *ipaccess.conf* file. If no client IP addresses appear (that is, the list is empty), connections from any MWTM client IP address are allowed.
- **rem**—Remove the specified client IP address from the *ipaccess.conf* file.
- **sample**—Print out a sample *ipaccess.conf* file.

Any changes you make take effect when you restart the MWTM server.

See [Implementing Secure User Access \(Server Only\)](#), page 2-2 for more information about using this command.

You must log in as the root user or superuser to use this command.

## mwtm jspport

### Server Only

### Full Syntax

**mwtm jspport** [*port-number*]

### Command Description

Sets a new port number for the JSP server, where *port-number* is the new, numeric port number. The MWTM verifies that the new port number is not already in use.

This command is needed only if you must change the port number after you install the MWTM; because another application must use the current port number.

The new port number must contain only numbers. If you enter a port number that contains nonnumeric characters, such as **mwtm13**, an error message appears, and the MWTM returns to the command prompt without changing the port number.

You must log in as the root user (not as a superuser) to use this command.

## mwtm keytool

### Solaris Server Only

### Full Syntax

**mwtm keytool** [**clear** | **genkey** | **import\_cert** *cert\_filename* | **import\_key** *key\_filename* *cert\_filename* | **list** | **print\_csr** | **print\_crt**]

**Command Description**

If you implement SSL in your MWTM system, manages SSL keys and certificates on the MWTM server.

If you installed the MWTM server and client on the same workstation, it also automatically manages the certificates on the client.

Use these keywords and arguments with this command:

- **clear**—Stops the MWTM server, if necessary, and removes all SSL keys and certificates from the server. Before restarting the server, you must either generate new SSL keys by using the **mwtm keytool genkey** command; or, you must completely disable SSL by using the **mwtm ssl disable** command.
- **genkey**—Stops the MWTM server, if necessary, and generates a new self-signed public or private SSL key pair on the MWTM server. The new keys take effect when you restart the server.
- **import\_cert** *cert\_filename*—Imports the specified signed SSL certificate in X.509 format.
- **import\_key** *key\_filename* *cert\_filename*—Imports the specified SSL key in OpenSSL format and the specified signed SSL certificate in X.509 format.
- **list**—Lists all SSL key-certificate pairs on the MWTM server.
- **print\_csr**—Prints a certificate signing request (CSR) in X.509 format.
- **print\_crt**—Prints the MWTM server's SSL certificate in X.509 format.

You must log in as the root user (not as a superuser) to use this command.

**Related Topic**

[Implementing SSL Support in the MWTM, page 2-22](#)

## mwtm killclients

**Server Only****Command Description**

Forcefully stops all MWTM clients on the local host, including all GTT clients and Event Editors.

You must log in as the root user (not as a superuser) to use this command.

## mwtm listusers

**Server Only****Full Syntax**

**mwtm listusers** [*username*]

**Command Description**

If you enable MWTM User-Based Access, lists all currently defined users in the authentication list, including this information for each user:

- User name.
- Last time the user logged in.

- User's authentication access level.
- User's current authentication status, such as **Account Enabled** or **Password Disabled**.

To list information for a specific user, use the *username* argument to specify the user.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Listing All Currently Defined Users \(Server Only\), page 2-18](#)

## mwtm logger

### Server Only

#### Command Description

Displays the system messages *messageLog.txt* file with tail -f.

To stop the display, press **Ctrl-C**.

## mwtm logincreds

### Server Only

#### Full Syntax

**mwtm logincreds** [**prompt** | **stored** | **status**]

#### Command Description

Requires the user to always provide credentials upon log in:

- **prompt**—User is always prompted for credentials in the following instances:
  - Running these commands—mwtm pushgtt, mwtm pushroute, mwtm pushmlr, and mwtm deployarchive
  - Deployment in the Route Table Editor, GTT Editor, and Address Table Editor
  - SSH connection protocol
  - Provisioning
- **stored**—If credentials are cached/configured, the user is not prompted to enter them. However, the user will be prompted if credentials are not cached or configured.
- **status**—Reflects the current status of the command (whether it is set to prompt or stored)

You must log in as the root user or superuser to use this command.

#### Related Topic

[Configuring Login Credentials, page 3-20](#)



# mwtm logsize

## Server Only

### Full Syntax

**mwtm logsize** [*number-of-lines*]

### Command Description

Sets the maximum size for truncating and rolling log files.

- Message log files are in *\$LOGDIR/messageLog-archives* (typically, */opt/CSCOs/gm/logs/messageLog-archives*).
- Network log files are in *\$LOGDIR/netStatus/archive*

If you enter this command without the *number-of-lines* argument, the MWTM displays the current maximum number of lines. You can then change that value or leave it (by pressing the Enter key).

The message and network log process archives the log file when the maximum number of lines is reached. The filename format of archived log files is:

messageLog.YYYY:MMDD:hhmm:y.txt.Z

or

networkLog.YYYY:MMDD:hhmm:y.txt.Z

where:

- *YYYY* is the year
- *MM* is the month in a two-digit format
- *DD* is the day of the month
- *hh* is the hour of the day in 24-hour notation
- *mm* is the minute within the hour
- *y* is one of these variables:

| Variable             | Meaning                                                                                                       | Example                                                                |
|----------------------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| r                    | The log file was created because the MWTM server restarted.                                                   | messageLog.2008:0328:1427:r.txt.Z<br>networkLog.2008:0328:1427:r.txt.Z |
| c                    | The log file was created because a user ran the <b>mwtm msglog clear</b> command.                             | messageLog.2008:0328:1433:c.txt.Z<br>networkLog.2008:0328:1433:c.txt.Z |
| o                    | The log file was created from a pre-existing <i>messageLog-old.txt</i> file (used in previous MWTM releases). | messageLog.2008:0328:1413:o.txt.Z<br>networkLog.2008:0328:1413:o.txt.Z |
| 0 (or higher number) | A counter that starts at 0 and increments sequentially. The number resets to 0 when the server restarts.      | messageLog.2008:0328:1427:3.txt.Z<br>networkLog.2008:0328:1427:3.txt.Z |

When *messageLog.txt* or *networkLog.txt* reaches the number of lines specified by the **mwtm logsize** command, the MWTM creates a new log archive file by using the filename format above. When the maximum number of lines is reached, the log filename contains a counter value to differentiate itself from other archived files (for example, *messageLog.2008:0328:1427:1.txt.Z* and *messageLog.2008:0328:1427:2.txt.Z*).

The default value for *number-of-lines* is 500,000 lines.

The valid range is 1,000 lines to an unlimited number of lines. The default value is 500,000 lines. If you specify a larger file size for the log file, the log file and its copy require proportionally more disk space.

When changing the number of lines to display, remember that every 5,000 lines require approximately 1 MB of disk space. You need to balance your need to refer to old messages against the amount of disk space they occupy.



#### Note

All log files are aged out by a timing mechanism (**mwtm msglogage**). You can estimate a size for the *\$LOGDIR/messageLog-archives* directory based on the number of lines, the amount of data that is logged (**mwtm mldebug**), and the log age.

You must log in as the root user or superuser to use this command. If you change the *number-of-lines* value, you must restart the server (**mwtm restart**).

## mwtm logtimemode

### Server Only

### Full Syntax

**mwtm logtimemode** [12 | 24]

### Command Description

Sets the time mode for dates in log files:

- **12**—Use 12-hour time, with AM and PM so that 1:00 in the afternoon is 1:00 PM.
- **24**—Use 24-hour time, also called military time so that 1:00 in the afternoon is 13:00. This is the default setting.

You must log in as the root user or superuser to use this command.

## mwtm manage

### Full Syntax

**mwtm manage** [itp | ipran | csg1 | csg2 | ggsn | bwg | ha] [enable | disable | status]

### Command Description

Enables, disables, or checks the status of managed network(s):

- **itp, ipran, csg1, csg2, ggsn, bwg, or ha**—Type of network.
- **disable**—Disables the MWTM from managing the chosen network.
- **enable**—Enables the MWTM to manage the chosen networks.
- **status**—Displays the status of networks (whether enabled or disabled).

You must log in as the root user or superuser to use this command.

## mwtm maxascirows

### Server Only

### Full Syntax

**mwtm maxascirows** [*number-of-rows*]

### Command Description

Sets the maximum number of rows for MWTM ASCII web output; for example, detailed debugging information.

If you enter this command without the *number-of-rows* argument, the MWTM displays the current maximum number of rows. You can then change that value or leave it. The valid range is 1 row to an unlimited number of rows. The default value is 6000 rows.

You must log in as the root user or superuser to use this command.

### Related Topic

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm maxevhist

### Server Only

### Full Syntax

**mwtm maxevhist** [*number-of-rows*]

### Command Description

Sets the maximum number of rows for the MWTM to search in the event history logs. The event history logs are the current and archived MWTM network status logs for status change and SNMP trap messages. The MWTM sends the results of the search to the web browser, where the setting of the *mwtm maxhtmlrows* command further limits the results.

If you enter this command without the *number-of-rows* argument, the MWTM displays the current maximum number of rows. You can then change that value or leave it. The valid range is 1 row to an unlimited number of rows. The default value is 15,000 rows.

The default setting is sufficient in most MWTM environments. However, you might need to increase the setting if the MWTM has archived a large number of event history logs, each log contains thousands of messages, and you want to search more than 15,000 rows. Remember that increasing this setting can increase the search time.

You must log in as the root user or superuser to use this command.

### Related Topic

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm maxhtmlrows

### Server Only

### Full Syntax

**mwtm maxhtmlrows** [*number-of-rows*]

### Command Description

Sets the maximum number of rows for MWTM HTML web output; for example, statistics reports, status change messages, or SNMP trap messages.



#### Note

If you have set the Page Size on the MWTM web interface, this command does not override that setting. When you set the Page Size feature on the MWTM web interface, browser cookies store the setting until the cookie expires or the MWTM deletes it.

If you enter this command without the *number-of-rows* argument, the MWTM displays the current maximum number of rows. You can then change that value or leave it. The valid range is 1 row to an unlimited number of rows. The default value is 200 rows.

You must log in as the root user or superuser to use this command.

### Related Topic

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm mldebug

### Server Only

### Full Syntax

**mwtm mldebug** [*mode*]

### Command Description

Sets the mode for logging MWTM debug messages:

- **normal**—Logs all action, error, and info messages. Use **mwtm mldebug normal** to revert to the default settings if you accidentally enter the **mwtm mldebug** command.
- **list**—Displays the current settings for the **mwtm mldebug** command.
- **all**—Logs all messages, of any type.
- **none**—Logs no messages at all.
- **minimal**—Logs all error messages.
- **action**—Logs all action messages.
- **debug**—Logs all debug messages.
- **dump**—Logs all dump messages.
- **error**—Logs all error messages.
- **info**—Logs all info messages.

- **NBAPI-SOAP**—Logs all northbound SOAP messages.
- **snmp**—Logs all SNMP messages.
- **trace**—Logs all trace messages.
- **trapsIn**—Logs all incoming trap messages.
- **trapsOut**—Logs all outgoing trap messages.

This command can adversely affect the MWTM performance. Use this command **only** under guidance from the Cisco Technical Assistance Center (TAC).

You must log in as the root user or superuser to use this command.

## mwtn modifysnmpcomm

### Full Syntax

**mwtn modifysnmpcomm -i *ipaddress* { -r *retry* | -t *timeout* | -p *poll* -c *community* }**

### Command Description

Modifies an existing SNMP configuration on the MWTM server.

- **-i *ipaddress***—the IP address of the device (required)
- At least one of the following:
  - **-r *retry***—the number of times to retry connecting to the device
  - **-t *timeout***—the timeout value, in seconds
  - **-p *poll***—the poll interval, in minutes
  - **-c *community***—the read community string of the device

You do not need to restart the MWTM server.

### Related Topic

- [mwtn addsnmpcomm, page B-6](#)
- [mwtn deletesnmpcomm, page B-24](#)
- [mwtn showsnmpcomm, page B-59](#)
- [mwtn snmpsetup, page B-65](#)

## mwtn motd

### Server Only

### Full Syntax

**mwtn motd [cat | disable | edit | enable]**

### Command Description

Manages the MWTM message of the day file, which is a user-specified MWTM system notice. You can set the message of the day to inform users of important changes or events in the MWTM system. The message of the day also provides users with the chance to exit the MWTM or GTT client before launching.

If you enable the message of the day, it appears whenever a user attempts to launch an MWTM or GTT client. If the user:

- Accepts the message, the client launches.
- Declines the message, the client does not launch.

Use these keywords with this command:

- **enable**—Enables the message of the day function. Initially, the message of the day file is blank; use the **mwtm motd edit** command to specify the message text.
- **edit**—Edits the message of the day.
- **cat**—Displays the contents of the message of the day file.
- **disable**—Disables this function (that is, stops displaying the message of the day whenever a user attempts to launch an MWTM or GTT client).

You must log in as the root user or superuser to use this command.

#### Related Topic

[Displaying a Message of the Day \(Server Only\), page 2-16](#)

## mwtm msglog

### Server Only

#### Full Syntax

**mwtm msglog** [**clear** | **-r**]

#### Command Description

Uses PAGER to display the contents of the system message log.

To save the current contents of the log, clear the log, and restart the server, enter **mwtm msglog clear**.

To display the contents of the log in reverse order, with the most recent messages at the beginning of the log, enter **mwtm msglog -r**.

You must log in as the root user or superuser to use this command.

## mwtm msglogage

### Server Only

#### Full Syntax

**mwtm msglogage** [*number-of-days*]

#### Command Description

Sets the maximum number of days to archive all types of log files before deleting them from the MWTM server.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 31 days.

The start date for aging out and deleting files is always yesterday at 12 AM. For example, say that you set the value to 1 day. You run the `mwtm msglogage` command at 3 PM on January 10th. To find files that will be deleted by the aging process, count back to 12 AM on January 10th, then add the number of days set in the command. In this example, we added 1 more day, so any file with an earlier timestamp than January 9th at 12 AM will be removed.

You must log in as the root user or superuser to use this command.

## mwtm msglogdir

### Server Only

### Full Syntax

**mwtm msglogdir** [*directory*]

### Command Description



#### Note

You must stop the MWTM server before performing this command. You are prompted whether to continue.

Changes the default location of all MWTM system message log files. By default, the system message log files reside on the MWTM server at `/opt/CSCOsgm/logs`.



#### Note

Do not set the new directory to any of these: `/usr`, `/var`, `/opt`, or `/tmp`. Also, do not set the new directory to the same directory in which you are storing GTT files (**mwtm gttdir**), report files (**mwtm repdir**), route table files (**mwtm routedir**), or address table files (**mwtm atbldir**).

After you change the directory, the MWTM asks if you want to restart the MWTM server. The new directory takes effect when you restart the MWTM server.

You must log in as the root user or superuser to use this command. If you change to a default location outside the MWTM, you must have appropriate permissions for that location.

## mwtm netlog

### Server Only

### Full Syntax

**mwtm netlog** [`clear` | `-r`]

### Command Description

Uses PAGER to display the contents of the network status log. To:

- Save the current contents of the log, clear the log, and restart the server, enter **mwtm netlog clear**.
- Display the contents of the log in reverse order, with the most recent network status messages at the beginning of the log, enter **mwtm netlog -r**.

You must log in as the root user or superuser to use this command.



## mwtm netlogger

### Server Only

#### Command Description

Displays the current contents of the network status log file with tail -f.

To stop the display, enter **Ctrl-c**.

## mwtm newlevel

### Server Only

#### Full Syntax

**mwtm newlevel** [*username*]

#### Command Description

If you enable MWTM User-Based Access, changes the authentication level for the specified user. Valid levels are:

- **1**—Basic User
- **2**—Power User
- **3**—Network Operator
- **4**—Network Administrator
- **5**—System Administrator

You must log in as the root user or superuser to use this command.

#### Related Topic

[Enabling and Changing Users and Passwords \(Server Only\), page 2-14](#)

## mwtm osinfo

### Server Only

#### Command Description

Depending on the network(s) that you have set, displays the operating system versions of software that the MWTM supports.

## mwtm passwordage



#### Note

You must have already changed your password at least once for this command to properly age the password.

### Server Only

#### Full Syntax

**mwtm passwordage** [*number-of-days* | **clear**]

#### Command Description

If you enable MWTM User-Based Access and you set **mwtm authtype** to **local**, number of days allowed before forcing users to change passwords. The number of days start to accrue beginning yesterday at 12 AM.



#### Note

For more details on how this works, see [mwtm msglogage](#), page B-45.

This function is disabled by default. If you do not specify this command, users will never need to change their passwords.

If you enter the **mwtm passwordage** command, the valid range is 1 day to an unlimited number of days. No default setting exists.

If you enabled this function and you want to disable it (that is, prevent the MWTM from forcing users to change passwords), enter **mwtm passwordage clear**.



#### Note

If **mwtm authtype** is set to **solaris**, you cannot use this command; instead, you must manage passwords on the external authentication servers.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Automatically Disabling Users and Passwords \(Server Only\)](#), page 2-11

## mwtm patchlog

### Server Only

#### Full Syntax

**mwtm patchlog**

#### Command Description

Uses PAGER to display the contents of the patch log, which lists the patches that you installed on the MWTM server.

The default path and filename for the patch log file is `/opt/CSCOsgm/install/sgmPatch.log`. If you installed the MWTM in a directory other than `/opt`, then the patch log file resides in that directory.

You must log in as the root user or superuser to use this command.

## mwtm poll

### Server Only

#### Full Syntax

**mwtm poll** [*node*] [*node*]...

#### Command Description

You use this command to poll one or more known nodes from the command line. Use the *node* arguments to specify the DNS names or IP addresses of one or more known nodes.

You must log in as the root user or superuser to use this command.

## mwtm pollertimeout

### Server Only

#### Full Syntax

**mwtm pollertimeout** [*number-of-seconds*]

#### Command Description

Specifies how long, in seconds, MWTM clients that are connected to the MWTM server can run a demand poller, as in a real-time data window or web page, before the MWTM automatically stops the poller to prevent unnecessary traffic on the network. When the demand poller times out, the MWTM stops the poller and sends an appropriate error message to the client.

The valid range is 1 second to an unlimited number of seconds. The default timeout is 8 hours (28800 seconds).

After you change the timeout, the MWTM asks if you want to restart the MWTM server. The new poller timeout takes effect when you restart the MWTM server.

See [Server Status Information:Pollers, page 5-45](#) for more information on demand pollers.

You must log in as the root user or superuser to use this command.

## mwtm print

### Server Only

#### Full Syntax

**mwtm print** {*all* | *device* | *snmp* | *task* | *alarmsummary*} [*severity*] [*quiet*]

#### Command Description

Displays information about device versions, SNMP settings, running tasks, summary of alarms, or all of this information.

Use these keywords with this command:

- **device**—Prints name, state, and system description of all nodes in the network.
- **snmp**—Prints SNMP information such as read and write community strings.

- **task**—Prints a list of task IDs and related information.
- **alarmsummary**—Prints a list of alarms sorted by severity types (critical, major, minor, and so on).
  - *severity*—Prints a list of alarms of a specified severity type. The *severity* takes one of these values: critical, major, minor, warning, informational, or indeterminate.
  - **quiet**—Use this keyword to print only the alarm counts (without the severity label)
- **all**—Prints the information available in all of the keywords of this command.

You must log in as the root user or superuser to use this command.

## mwtm props

### Server and Solaris or Linux Clients Only

#### Command Description

Displays the contents of the *System.properties* files for both MWTM server and client installs.

You must log in as the root user or superuser to use this command.

## mwtm provisiontool

### Server Only

#### Full Syntax

**mwtm provisiontool -a** *actionName* [*parameters*]

#### Command Description

Invokes provisioning API operations.

You can specify these action names (and any corresponding required parameters) by using the **-a** option:

| Option | Action Names      | Parameters                 |
|--------|-------------------|----------------------------|
| -a     | provision         | -r<br>-H<br>-p<br>-S<br>-h |
|        | syncFromDevice    | -f                         |
|        | iosWriteToStartup | -H<br>-p<br>-S<br>-h       |

You can use these parameters:

| Parameter | Description                                                                                                                                                                   |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r        | Specifies a file name for <b>ProvisionRequest</b> , which is an XML element from the MWTM WSDL definitions.                                                                   |
| -f        | Specifies a fully qualified domain name (FQDN).                                                                                                                               |
| -H        | (Optional) Specifies a hostname to connect to. If unspecified, the system obtains the default value from the MWTM server <i>System.properties</i> file, SERVER_NAME property. |
| -p        | (Optional) Specifies a port to which to connect. If unspecified, the system obtains the default value from the MWTM server <i>System.properties</i> file, WEB_PORT property.  |
| -S        | (Optional) Specifies whether to use SSL (https) for NBAPI access. The default is no SSL.                                                                                      |
| -h        | (Optional) Print help information.                                                                                                                                            |

You must log in as the root user or superuser to use this command.

#### Related Documentation

See the *Cisco Mobile Wireless Transport Manager 6.1 OSS Integration Guide*.

[http://cisco.com/en/US/docs/net\\_mgmt/mobile\\_wireless\\_transport\\_manager/6.1/installation/guide/mwtmig.html](http://cisco.com/en/US/docs/net_mgmt/mobile_wireless_transport_manager/6.1/installation/guide/mwtmig.html)

## mwtm purgedb

### Server Only

#### Command Description

Permanently deletes all components in the MWTM database marked for deletion.

The MWTM keeps information about older objects in its database even after they have been deleted. This is considered a logically deleted state. MWTM retains this information to try and maintain any user customized data associated with an object (for instance, a customized name) in case the object is rediscovered at some point in the future. Logically deleted data is physically deleted after seven days if it is not reused by then. You can use the `mwtm purgedb` command to immediately remove this logically deleted data from the MWTM database.

Unfortunately, this benefit may have a side effect. In certain cases, rediscovery of a deleted object may cause the MWTM to use obsolete information in the database, rather than the new information. Ultimately, some configuration changes are not detected, and the viewable data from the client application is incorrect.



#### Note

The `mwtm purgedb` command does not cause the loss of any collected statistical data.

You must log in as the root user or superuser to use this command.

## mwtm readme

### Server and Solaris or Linux Clients Only

#### Command Description

Displays the contents of the README file for the MWTM.

#### Related Topic

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm reboot

### Server Only

#### Command Description

Reboots the Solaris MWTM system.



#### Note

Use this command with care. Rebooting the Solaris MWTM system disconnects all MWTM clients that are using the system. Before using this command, use the **mwtm who** command to list all current users; and, the **mwtm wall** command to warn all current users that you are rebooting the system.

You must log in as the root user (not as a superuser) to use this command.

## mwtm repdailyage

### Server Only

#### Full Syntax

**mwtm repdailyage** [*number-of-days*]

#### Command Description

Maximum number of days the MWTM should archive daily reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 90 days.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm rephelp

### Server Only

#### Command Description

Displays help for all commands that are related to MWTM reports.

You must log in as the root user or superuser to use this command.

## mwtm rephourlyage

### Server Only

#### Full Syntax

**mwtm rephourlyage** [*number-of-days*]

#### Command Description

Maximum number of days the MWTM should archive hourly reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 31 days.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm restart

### Server Only

#### Full Syntax

**mwtm restart** [**jsp** | **pm** | **web**]

#### Command Description

Restarts MWTM servers on the local host:

- **jsp**—Restarts the MWTM JSP Server.
- **pm**—Restarts the MWTM Application Server and all managed processes.
- **web**—Restarts the MWTM web Server.

If you do not specify a keyword, **mwtm restart** restarts all MWTM servers.

You must log in as the root user or superuser to use this command.

## mwtm restore

### Server Only

#### Full Syntax

**mwtm restore** [**archive** | **atbl** | **gtt** | **logs** | **reports** | **routes** | **security**]

#### Command Description

Restores the MWTM data files from a previous backup, stored in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the locations of the backup files are */opt/mwmtm61-client-backup.tar.Z* and */opt/mwmtm61-server-backup.tar.Z*.
- A different directory, then the backup files reside in that directory.

You can restore data files on the same Solaris or Linux server; or, on a different Solaris or Linux server that is running MWTM 6.1.

To restore only specific parts of the MWTM data files, use these keywords:

- **archive**—Restores the MWTM archive repository.
- **atbl**—Restores only MWTM Address Table Editor files.
- **gtt**—Restores only MWTM GTT files.
- **logs**—Restores only MWTM log files, such as the message log files.
- **reports**—Restores only MWTM report files, such as the statistics report files.
- **routes**—Restores only MWTM ITP route table files.
- **security**—Restores only the security-related parts of the MWTM data files. This command is useful if you inadvertently delete your user accounts or make other unwanted changes to your MWTM security information.



#### Note

If **mwtm backupdays** was previously used to set the number of backup days to more than one day, the **mwtm restore** command will prompt you for a server or client backup file to restore from (because there would be more than one backup file to choose from).

To change the directory in which the MWTM stores these backup files, use the **mwtm backupdir** command.

You must log in as the root user (not as a superuser) to use this command.

#### Related Topic

- [Backing Up or Restoring MWTM Files \(Server Only\)](#), page 2-32
- [mwtm backupdays](#), page B-9
- [mwtm backupdir](#), page B-10



## mwtm restoreprops

### Server and Solaris or Linux Clients Only

#### Command Description

Restores the MWTM server and client *System.properties* files and other important configuration files to the backup versions of the files.

You must log in as the root user (not as a superuser) to use this command.

## mwtm rootvars

### Server and Solaris or Linux Clients Only

#### Command Description

Displays the contents of the */etc/CSCOsgm.sh* file, which determines the root location of the MWTM server and client installation.

## mwtm sechelp

### Server Only

#### Command Description

Displays help for all commands that are related to MWTM security.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Chapter 2, “Configuring Security”](#)

## mwtm seclog

### Server Only

#### Full Syntax

**mwtm seclog** [clear | -r]

#### Command Description

Uses PAGER to display the contents of the system security log.

These security events are recorded in the log:

- All changes to system security, including adding users.
- Log-in attempts, whether successful or unsuccessful, and logoffs.
- Attempts to switch to another user's account, whether successful or unsuccessful.
- Attempts to access files or resources of higher authentication level.
- Access to all privileged files and processes.

- Operating system configuration changes and program changes, at the Solaris level.
- The MWTM restarts.
- Failures of computers, programs, communications, and operations, at the Solaris level.

To clear the log, enter **mwtm seclog clear**.

To display the contents of the log in reverse order, with the most recent security events at the beginning of the log, enter **mwtm seclog -r**.

The default path and filename for the system security log file is */opt/CSCOs/gm/logs/sgmSecurityLog.txt*. If you installed the MWTM in a directory other than */opt*, then the system security log file resides in that directory.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Displaying the Contents of the System Security Log \(Server Only\), page 2-18](#)

## mwtm secondaryserver

### Server Only

#### Full Syntax

**mwtm secondaryserver** [*hostname naming-port webport*] | [**list**] | [**clear**]

#### Command Description

Configures a secondary MWTM server, where:

- *hostname* is the name of the host on which you installed the secondary MWTM server.
- *naming-port* is the MWTM Naming Server port number for the secondary MWTM server. The default port number is 44742.
- *webport* is the MWTM web port number for the secondary MWTM server. The default port number is 1774.

For best results, Cisco recommends that you configure the primary server and the secondary server as secondaries for each other.

If you use the **mwtm secondaryserver** command to configure a secondary MWTM server, but the primary MWTM server fails before you launch the MWTM client, the MWTM client does not detect the secondary server.

To list the secondary MWTM server that you configured for this primary MWTM server, enter the **mwtm secondaryserver list** command. If a secondary server is not yet configured, an informative message appears.

To remove the current settings for the secondary server, enter the **mwtm secondaryserver clear** command. This command stops the server and removes the current values for these properties in the *System.properties* file:

- BACKUP\_SERVER
- BACKUP\_RMIPORT
- BACKUP\_WEBPORT

The **mwtm secondaryserver clear** command also restarts the server to activate the changes.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Configuring a Backup MWTM Server, page 3-10](#)

## mwtm servername

**Server and Solaris or Linux Clients Only****Full Syntax**

**mwtm servername** [*hostname*]

**Command Description**

Resets the MWTM server's default hostname, where *hostname* is the new default hostname:

- Ensure that the new default hostname is valid and defined in your */etc/hosts* file. If not, you might not be able to start the MWTM server.
- If you are not logged in as the root user or as a superuser when you enter this command from an MWTM client, the default hostname changes only for that MWTM client and the user who entered the command.
- If you are logged in as the root user or superuser when you enter this command, the default hostname changes for the MWTM server and client, and it restarts the MWTM server. The MWTM server uses the new default hostname to register RMI services, and MWTM clients use the new default hostname to connect to the server.
- If you are logged into a *client-only* installation as the root user or as a superuser when you enter this command, the default hostname changes only for that MWTM client. The MWTM client uses the new default hostname to connect to the MWTM server.

**Note**

Using the **mwtm servername** command to reset the MWTM server's default hostname does not affect communication between the MWTM server and the ITPs.

**Related Topic**

- [Appendix C, “FAQs”](#)
- [Appendix H, “Configuring MWTM to Run with Various Networking Options”](#)

## mwtm setpath

**Server and Solaris or Linux Clients Only****Full Syntax**

**mwtm setpath** [*username*]

**Command Description**

Appends binary (*bin*) directories to the path for a user. Users can then append the proper MWTM binary directories to their paths without manually editing the *.profile* and *.cshrc* files.

This command appends lines such as these to the user's *.profile* file:

```
PATH=$PATH:/opt/CSCOsgm/bin:/opt/CSCOsgmClient/bin # CiscoSGM
```

and appends lines such as these to the user's *.cshrc* file:

```
set path=($path /opt/CSCOsgm/bin /opt/CSCOsgmClient/bin) # CiscoSGM
```

Thereafter, you can enter MWTM commands as:

```
mwtm help
```

instead of:

```
/opt/CSCOsgm/bin/mwtm help
```

When entering this command, remember that:

- If you enter this command and you do not specify a *username*, the MWTM appends the *bin* directories to your path (that is, to the path for the user who is currently logged in and entering the **mwtm setpath** command).
- If you enter this command and you specify a *username*, the MWTM appends the *bin* directories to the path for the specified user. To specify a *username*, follow these conditions:
  - You must log in as the root user.
  - The specified *username* must exist in the local */etc/passwd* file.
  - You cannot specify a *username* that is defined in a distributed Network Information Services (NIS) system or in an Network File System-mounted (NFS-mounted) home directory.
- If you enter this command more than once for the same user, each command overwrites the previous command. The MWTM does not append multiple *bin* directories to the same path.
- You might have to use the **su** - command when you enter root-level commands. If you use the **su** command to become the root user, rather than logging in as the root user, then you must use the - option.

## mwtm showcreds

### Server Only

### Full Syntax

**mwtm showcreds** [-i *ipaddress*] [-d *nodetype*]

### Command Description

Displays credentials for a given IP address, if specified. Otherwise, the Default credentials are used. To:

- Display credentials for a particular IP address only, use **-i** and the IP address of the node.
- Add credentials for a specific node type, specify **-d** and the nodetype, which can be:
  - **itp**—ITP nodes.
  - **ons**—ONS nodes.
  - **csr**—Cell Site Router (CSR) nodes.
  - **ran\_svc**—RAN\_SVC nodes.

You must log in as the root user or superuser to use this command.

### Related Topic

[Credentials Commands, page 3-23](#)

## mwtm showsnmpcomm

### Full Syntax

**mwtm showsnmpcomm** [-i *ipaddress*]

### Command Description

Shows the specified SNMP configuration, or all SNMP configurations, on the MWTM server.

**-i ipaddress**—the IP address of the device (optional). If not specified, displays all SNMP configurations on the server.

### Related Topic

- [mwtm addsnmpcomm, page B-6](#)
- [mwtm deletesnmpcomm, page B-24](#)
- [mwtm modifiesnmpcomm, page B-44](#)
- [mwtm snmpsetup, page B-65](#)

## mwtm snmpcomm

### Server Only

### Full Syntax

**mwtm snmpcomm** [*name*]

**Command Description**

You use this command to set a new default SNMP read community name. The MWTM automatically updates the name in the SNMP parameters file. The default path and filename for the SNMP parameters file is */opt/CSCOsgm/etc/communities.conf*.

You must log in as the root user or superuser to use this command.

**Related Topic**

[SNMP Configuration Commands, page 3-18](#)

## mwtm snmpconf

**Server Only****Full Syntax**

**mwtm snmpconf** [*filename*]

**Command Description**

Sets the file used for SNMP parameters, such as community names, timeouts, and retries.

The default path and filename for the SNMP parameters file is */opt/CSCOsgm/etc/communities.conf*. If you installed the MWTM in a directory other than */opt*, then the file resides in that directory.

When you specify a new path or filename, the MWTM restarts the servers.

**Note**

The SNMP parameters file uses the HP OpenView format; therefore, you can set this path and filename to point to the HP OpenView *ovsnmp.conf* file in an existing OpenView system. For information about exporting SNMP community names from CiscoWorks Resource Manager Essentials (RME), see [Importing SNMP Community Names from CiscoWorks \(Solaris Only\), page 3-2](#).

You must log in as the root user or superuser to use this command.

**Related Topic**

[SNMP Configuration Commands, page 3-18](#)

## mwtm snmpget

**Server Only****Full Syntax**

**mwtm snmpget** [-JJVM\_ARG1 [-JJVM\_ARG2]...] [-v *snmp\_version*] [-c *community\_string*] [-r *retry*] [-t *timeout*] [-d *output\_delimiter*] [--header|--no-header] [--raw-octets|--no-raw-octets] [--str-octets|--no-str-octets] [--raw-timeticks|--no-raw-timeticks] [--resolve-integer|--no-resolve-integer] [--resolve-bits|--no-resolve-bits] [--get-sysuptime|--no-get-sysuptime] [--detect-mib-error] [--instance *oids*] [--int-instance *integer*] [--str-instance *string*] [*hostname*] [*oid*] [*oid*]...

**Command Description**

Queries the specified *hostname* by using SNMP **GetRequests**. Use these optional keywords and arguments with this command:

- **-JJVM\_ARG1**—JVM options. You must specify the **-J** keyword and arguments before any other keywords and arguments.

For example, by default JVM uses a maximum of 64 MB of memory; however, if you are walking a large table, JVM might require more memory. To enable JVM to use a maximum of 256 MB of memory, use this syntax:

**-J-Xmx256m**

- **-v snmp\_version**—SNMP protocol version. Valid versions are **1** or **2c**. The default version is **2c**.
- **-c community\_string**—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-r retry**—SNMP retry count. You specify the default retry count in the SNMP parameters file, *communities.conf*.
- **-t timeout**—SNMP timeout, in seconds. You specify the default timeout in the SNMP parameters file, *communities.conf*.
- **-d output\_delimiter**—Output delimiter. The default output delimiter is a colon (:).
- **--header|--no-header**—Specifies whether to display variable names as table headers:
  - Specify **--header** to display variable names as table headers for tabular output, or to display MIB variable OIDs with the value for nontabular output. This is the default setting.
  - Specify **--no-header** if you do not want to display variable names as table headers for tabular output, or MIB variable OIDs with the value for nontabular output.
- **--raw-octets|--no-raw-octets**—Specifies whether to display octets as raw octets:
  - Specify **--raw-octets** to display raw octets, such as **6c 69 6e 6b**, for octet strings.
  - Specify **--no-raw-octets** if you do not want to display raw octets for octet strings. This is the default setting.

The other option for displaying octets is **--str-octets|--no-str-octets**.

- **--str-octets|--no-str-octets**—Specifies whether to display octets as strings:
  - Specify **--str-octets** to display octets as strings, such as **link**. This is the default setting.
  - Specify **--no-str-octets** if you do not want to display octets as strings.

The other option for displaying octets is **--raw-octets|--no-raw-octets**.

- **--raw-timeticks|--no-raw-timeticks**—Specifies the time format:
  - Specify **--raw-timeticks** to specify raw timeticks, such as **2313894**.
  - Specify **--no-raw-timeticks** to specify formatted timeticks, such as **6 Hours 26 Mins 12 Secs**. This is the default setting.
- **--resolve-integer|--no-resolve-integer**—Specifies the time format. Use:
  - **--resolve-integer** to display integers using the string description in the MIB, such as **available** or **unavailable**.
  - **--no-resolve-integer** to display integers as numbers. This is the default setting.
- **--resolve-bits|--no-resolve-bits**—Specifies the time format. Use:

- **--resolve-bits** to display bits using the string description in the MIB, such as **continue** or **ruleset**.
- **--no-resolve-bits** to display bits as numbers, such as **1** or **14**. This is the default setting.
- **--get-sysuptime|--no-get-sysuptime**—Specifies whether to retrieve the **sysuptime**. Use:
  - **--get-sysuptime** to retrieve the sysuptime in the same packet as each SNMP operation.
  - **--no-get-sysuptime** if you do not want to retrieve the sysuptime in the same packet. This is the default setting.
- **--detect-mib-error**—Detects errors in returned MIB variables, such as **noSuchInstance**, **noSuchObject**, and **endOfMibView**. If the system detects any such errors, an error message and error code appear.

Sometimes multiple MIB variables are returned at the same time, some of which are in error; others are not. If this occurs and you:

- Specified **--detect-mib-error**, none of the correct values appear, only the error message, and it returns an error code.
- Did not specify **--detect-mib-error**, a return code of 0 is returned and all MIB variables appear. (Even **noSuchInstance** appears as a returned value.) This is the default setting, with **--detect-mib-error** not specified.
- **--instance oids**—Appends instance OIDs to each polling MIB variable. For example, these commands perform the same function:

```
mwtm snmpget --instance 172.18.16.10 node_1 ipAdEntIfIndex ipAdEntNetMask
```

```
mwtm snmpget node_1 ipAdEntIfIndex.172.18.16.10 ipAdEntNetMask.172.18.16.10
```

- **--int-instance integer**—Appends the specified integer instance OID to each polling MIB variable.
- **--str-instance string**—Appends string instance OIDs to each polling MIB variable; for example, these commands perform the same function:

```
mwtm snmpget --str-instance link_1 node_1 cItpSpLinksetState
```

```
mwtm snmpget node_1 cItpSpLinksetState.6.108.115.110.97.109.101
```

- *hostname*—Name of the host to query.
- *oid*—One or more OIDs or variable names.

The default path for the SNMP parameters file, *communities.conf*, is */opt/CSCOs/gm/etc/communities.conf*. If you installed the MWTM in a directory other than */opt*, then the file resides in that directory. You can edit the file manually or using the MWTM client (see [Launching the Discovery Dialog](#), page 4-6).

You must log in as the root user or superuser to use this command.

#### Related Topic

[SNMP Configuration Commands](#), page 3-18



## mwtm snmphelp

### Server Only

#### Command Description

Displays help for all commands that are related to SNMP queries.

You must log in as the root user or superuser to use this command.

#### Related Topic

[SNMP Configuration Commands, page 3-18](#)

## mwtm snmpmaxrows

### Server Only

#### Full Syntax

**mwtm snmpmaxrows** [*number-of-rows*]

#### Command Description

Sets the value of maximum rows for SNMP walk.

The MWTM collects network information from device MIBs using SNMP protocol. In certain ITP networks, some MIB tables can be very large (such as GTT tables, MTP3 accounting statistics tables, etc.) The default value of 100,000 rows is usually sufficient even for large networks. However, for very large networks, if the limit needs to be increased, you can customize the this parameter. It is not recommended to exceed 300,000 rows.

If you enter this command without the *number-of-rows* argument, the MWTM displays the current maximum number of rows. You can then change that value or leave it. The valid range is 1 row to an unlimited number of rows; however, it is not recommended to set this number at less than 10,000. The default value is 100,000 rows.

You must log in as the root user or superuser to use this command.

## mwtm snmpnext

### Server Only

#### Full Syntax

**mwtm snmpnext** [-JVM\_ARG1 [-JVM\_ARG2]...] [-v *snmp\_version*] [-c *community\_string*] [-r *retry*] [-t *timeout*] [-d *output\_delimiter*] [--header|--no-header] [--raw-octets|--no-raw-octets] [--str-octets|--no-str-octets] [--raw-timeticks|--no-raw-timeticks] [--resolve-integer|--no-resolve-integer] [--resolve-bits|--no-resolve-bits] [--get-sysuptime|--no-get-sysuptime] [--detect-mib-error] [--instance *oids*] [--int-instance *integer*] [--str-instance *string*] [*hostname*] [*oid*] [*oid*]...

#### Command Description

Queries the specified *hostname* by using SNMP **GetNextRequests**. Use these optional keywords and arguments with this command:

- **-JVM\_ARG1**—JVM options. You must specify the **-J** keyword and arguments before any other keywords and arguments.

For example, by default JVM uses a maximum of 64 MB of memory; however, if you explore a large table, JVM might require more memory. To enable JVM to use a maximum of 256 MB of memory, use this option:

**-J-Xmx256m**

- **-v snmp\_version**—SNMP protocol version. Valid versions are **1** or **2c**. The default version is **2c**.
- **-c community\_string**—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-r retry**—SNMP retry count. You specify the default retry count in the SNMP parameters file, *communities.conf*.
- **-t timeout**—SNMP timeout, in seconds. You specify the default timeout in the SNMP parameters file, *communities.conf*.
- **-d output\_delimiter**—Output delimiter. The default output delimiter is a colon (:).
- **--header|--no-header**—Specifies whether to display variable names as table headers:
  - Specify **--header** to display variable names as table headers for tabular output or MIB variable OIDs with the value for nontabular output. This is the default setting.
  - Specify **--no-header** if you do not want to display variable names as table headers for tabular output or MIB variable OIDs with the value for nontabular output.
- **--raw-octets|--no-raw-octets**—Specifies whether to display octets as raw octets. Use:
  - **--raw-octets** to display raw octets, such as **6c 69 6e 6b**, for octet strings.
  - **--no-raw-octets** if you do not want to display raw octets for octet strings. This is the default setting.

The other option for displaying octets is **--str-octets|--no-str-octets**.

- **--str-octets|--no-str-octets**—Specifies whether to display octets as strings. Use:
  - **--str-octets** to display octets as strings, such as **link**. This is the default setting.
  - **--no-str-octets** if you do not want to display octets as strings.
- **--raw-timeticks|--no-raw-timeticks**—Specifies the time format:
  - Specify **--raw-timeticks** to specify raw timeticks, such as **2313894**.
  - Specify **--no-raw-timeticks** to specify formatted timeticks, such as **6 Hours 26 Mins 12 Secs**. This is the default setting.
- **--resolve-integer|--no-resolve-integer**—Specifies the time format. Use:
  - **--resolve-integer** to display integers using the string description in the MIB, such as **available** or **unavailable**.
  - **--no-resolve-integer** to display integers as numbers. This is the default setting.
- **--resolve-bits|--no-resolve-bits**—Specifies the time format:
  - Specify **--resolve-bits** to display bits using the string description in the MIB, such as **continue** or **ruleset**.
  - Specify **--no-resolve-bits** to display bits as numbers, such as **1** or **14**. This is the default setting.

- **--get-sysuptime|--no-get-sysuptime**—Specifies whether to retrieve the **sysuptime**. Use:
  - **--get-sysuptime** to retrieve the sysuptime in the same packet as each SNMP operation.
  - **--no-get-sysuptime** if you do not want to retrieve the sysuptime in the same packet. This is the default setting.
- **--detect-mib-error**—Detects errors in returned MIB variables, such as **noSuchInstance**, **noSuchObject**, and **endOfMibView**. If the system detects any such errors, an error message appears and an error code is returned.

Sometimes multiple MIB variables are returned at the same time, some of which are in error; others are not. If this occurs and you:

- Specified **--detect-mib-error**, none of the correct values appear, only the error message and it returns an error code.
  - Did not specify **--detect-mib-error**, a return code of 0 is returned and all MIB variables appear (even **noSuchInstance** appears as a returned value). This is the default setting, with **--detect-mib-error** not specified.
- **--instance *oids***—Appends instance OIDs to each polling MIB variable. For example, these commands perform the same function:

```
mwtm snmpget --instance 172.18.16.10 node_1 ipAdEntIfIndex ipAdEntNetMask
```

```
mwtm snmpget node_1 ipAdEntIfIndex.172.18.16.10 ipAdEntNetMask.172.18.16.10
```

- **--int-instance *integer***—Appends the specified integer instance OID to each polling MIB variable.
- **--str-instance *string***—Appends string instance OIDs to each polling MIB variable. For example, these commands perform the same function:

```
mwtm snmpget --str-instance link_1 node_1 cItpSpLinksetState
```

```
mwtm snmpget node_1 cItpSpLinksetState.6.108.115.110.97.109.101
```

- *hostname*—Name of the host to be queried.
- *oid*—One or more OIDs or variable names.

The default path for the SNMP parameters file, *communities.conf*, is */opt/CSCOs/gm/etc/communities.conf*. If you installed the MWTM in a directory other than */opt*, then the file resides in that directory. You can edit the file manually or by using the MWTM client (see [Launching the Discovery Dialog](#), page 4-6).

You must log in as the root user or superuser to use this command.

#### Related Topic

[SNMP Configuration Commands](#), page 3-18

## mwtm snmpsetup

### Server Only

### Full Syntax

```
mwtm snmpsetup
```

**Command Description**

Sets up SNMP configurations on the MWTM server for multiple devices and optionally discovers the new nodes. This command interactively prompts you to add, modify, or delete one or more SNMP configurations, which include values for:

- Hostname
- Read community string
- Poll interval (in minutes)
- Timeout (in seconds)
- Number of retries

When modifying poll interval, retry, and timeout values, this command displays the currently available value in brackets [ ]. When adding new SNMP configurations, this command displays default values.

After adding, modifying, or deleting an SNMP configuration, this command prompts you to discover the node (only this node is discovered).

You do not need to restart the server when using this command.

**Related Topic**

- [mwtm addsnmpcomm](#), page B-6
- [mwtm deletesnmpcomm](#), page B-24
- [mwtm modifiesnmpcomm](#), page B-44
- [mwtm showsnmpcomm](#), page B-59

## mwtm snmpwalk

**Server Only****Full Syntax**

```
mwtm snmpwalk [-JJVM_ARG1 [-JJVM_ARG2]...] [-v snmp_version] [-c community_string]
[-r retry] [-t timeout] [-x maximum_rows] [-d output_delimiter] [--tabular|--no-tabular]
[--getbulk|--no-getbulk] [--header|--no-header] [--raw-octets|--no-raw-octets]
[--str-octets|--no-str-octets] [--raw-timeticks|--no-raw-timeticks]
[--resolve-integer|--no-resolve-integer] [--resolve-bits|--no-resolve-bits]
[--get-sysuptime|--no-get-sysuptime] [--detect-mib-error] [--instance oids] [--int-instance integer]
[--str-instance string] [hostname] [oid] [oid]...
```

**Command Description**

Queries the specified *hostname* by using SNMP **GetNextRequests** to go through the MIB. Use these optional keywords and arguments with this command:

- **-JJVM\_ARG1**—JVM options. You must specify the **-J** keyword and arguments before any other keywords and arguments.

For example, by default JVM uses a maximum of 64 MB of memory; however, if you are going through a large table, JVM might require more memory. To enable JVM to use a maximum of 256 MB of memory, use this option:

```
-J-Xmx256m
```

- **-v *snmp\_version***—SNMP protocol version. Valid versions are **1** or **2c**. The default version is **2c**.
- **-c *community\_string***—SNMP community string. You specify the default community string in the SNMP parameters file, *communities.conf*.
- **-r *retry***—SNMP retry count. You specify the default retry count in the SNMP parameters file, *communities.conf*.
- **-t *timeout***—SNMP timeout, in seconds. You specify the default timeout in the SNMP parameters file, *communities.conf*.
- **-x *maximum\_rows***—Maximum number of rows to go through. If a table has more than the maximum number of rows, the **mwtn snmpwalk** command fails. You can use the **-m** keyword and argument to increase the maximum number of rows to go through. The default setting is 10,000 rows.

However, for every 10,000 rows gone through, JVM requires an additional 10 MB of memory. You can use the **-J** keyword and argument to increase the memory available to JVM.

- **-d *output\_delimiter***—Output delimiter. The default output delimiter is a colon (:).
- **--tabular|--no-tabular**—Specifies whether to print the result of the query in tabular format. Use:
  - **--tabular** to print the result in tabular format. This is the default setting.
  - **--no-tabular** if you do not want to print the result in tabular format.
- **--getbulk|--no-getbulk**—(SNMP version 2c only) Specifies whether to use the **getbulk** command to go through the table. Use:
  - **--getbulk** to use the **getbulk** command. This is the default setting.
  - **--no-getbulk** if you do not want to use the **getbulk** command.
- **--header|--no-header**—Specifies whether to display variable names as table headers. Use:
  - **--header** to display variable names as table headers for tabular output or to display MIB variable OIDs with the value for nontabular output. This is the default setting.
  - **--no-header** if you do not want to display variable names as table headers for tabular output or MIB variable OIDs with the value for nontabular output.
- **--raw-octets|--no-raw-octets**—Specifies whether to display octets as raw octets. Use:
  - **--raw-octets** to display raw octets, such as **6c 69 6e 6b**, for octet strings.
  - **--no-raw-octets** if you do not want to display raw octets for octet strings. This is the default setting.

The other option for displaying octets is **--str-octets|--no-str-octets**.

- **--str-octets|--no-str-octets**—Specifies whether to display octets as strings. Use:
  - **--str-octets** to display octets as strings, such as **link**. This is the default setting.
  - **--no-str-octets** if you do not want to display octets as strings.

The other option for displaying octets is **--raw-octets|--no-raw-octets**.

- **--raw-timeticks|--no-raw-timeticks**—Specifies the time format. Use:
  - **--raw-timeticks** to specify raw timeticks, such as **2313894**.
  - **--no-raw-timeticks** to specify formatted timeticks, such as **6 Hours 26 Mins 12 Secs**. This is the default setting.
- **--resolve-integer|--no-resolve-integer**—Specifies the time format. Use:
  - **--resolve-integer** to display integers using the string description in the MIB, such as **available** or **unavailable**.

- **--no-resolve-integer** to display integers as numbers. This is the default setting.
- **--resolve-bits|--no-resolve-bits**—Specifies the time format. Use:
  - **--resolve-bits** to display bits using the string description in the MIB, such as **continue** or **ruleset**.
  - **--no-resolve-bits** to display bits as numbers, such as **1** or **14**. This is the default setting.
- **--get-sysuptime|--no-get-sysuptime**—Specifies whether to retrieve the sysuptime. Use:
  - **--get-sysuptime** to retrieve the sysuptime in the same packet as each SNMP operation.
  - **--no-get-sysuptime** if you do not want to retrieve the **sysuptime** in the same packet. This is the default setting.

- **--detect-mib-error**—Detects errors in returned MIB variables, such as **noSuchInstance**, **noSuchObject**, and **endOfMibView**. If the system detects any such errors, an error message and error code appear.

Sometimes multiple MIB variables are returned at the same time, some of which are in error; others are not. If this occurs and you:

- Specified **--detect-mib-error**, none of the correct values appear, only the error message and an error code is returned.
- Did not specify **--detect-mib-error**, a return code of 0 and all MIB variables appear; even **noSuchInstance** appears as a returned value. This is the default setting, with **--detect-mib-error** not specified.
- **--instance *oids***—Appends instance OIDs to each polling MIB variable. For example, these commands perform the same function:

```
mwtm snmpget --instance 172.18.16.10 node_1 ipAdEntIfIndex ipAdEntNetMask
```

```
mwtm snmpget node_1 ipAdEntIfIndex.172.18.16.10 ipAdEntNetMask.172.18.16.10
```

- **--int-instance *integer***—Appends the specified integer instance OID to each polling MIB variable.
- **--str-instance *string***—Appends string instance OIDs to each polling MIB variable. For example, these commands perform the same function:

```
mwtm snmpget --str-instance link_1 node_1 cItpSpLinksetState
```

```
mwtm snmpget node_1 cItpSpLinksetState.6.108.115.110.97.109.101
```

- *hostname*—Name of the host to query.
- *oid*—One or more OIDs or variable names.

The default path for the SNMP parameters file, *communities.conf*, is */opt/CSCOs/gm/etc/communities.conf*. If you installed the MWTM in a directory other than */opt*, then the file resides in that directory. You can edit the file manually or using the MWTM client (see [Launching the Discovery Dialog, page 4-6](#)).

You must log in as the root user or superuser to use this command.

#### Related Topic

[SNMP Configuration Commands, page 3-18](#)

## mwtm sounddir

### Server Only

### Full Syntax

```
mwtm sounddir [directory]
```

### Command Description



#### Note

You must stop the MWTM server before performing this command. You are prompted whether to continue.

Sets the directory in which the MWTM server stores event automation sound files (see [Changing the Way the MWTM Processes Events, page 9-35](#) for information about sound files).

The default directory for sound files resides in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the default directory is */opt/CSCOs/gm/sounds*.
- A different directory, then the default directory resides in that directory.

Use this command if you want to use a different directory for MWTM server event automation sound files, such as a Network File System location on another server.

**Note**

This command copies all files in the current directory to the new directory. If you are not logged in as the superuser and you do not own the new directory, you might not be able to copy the files. In that case, you must specify a directory that you own, or you must log in as the root user.

You must log in as the root user to use this command.

## mwtm ssl

### Server Only

### Full Syntax

**mwtm ssl** [**enable** | **disable** | **status**]

### Command Description

If you enable the SSL on the MWTM and you have an SSL key-certificate pair on the MWTM, you can use this command to manage SSL support in the MWTM:

- **enable**—Enables SSL support.
- **disable**—Disables SSL support.
- **status**—Displays the current status of SSL support in the MWTM, including whether you enabled or disabled SSL support, and which SSL keys and certificates exist.

You must log in as the root user (not as a superuser) to use this command.

### Related Topic

[Implementing SSL Support in the MWTM, page 2-22](#)



## mwtm sslstatus

### Server Only

#### Command Description

Displays the current status for SSL that the MWTM supports, including whether you enabled or disabled SSL support; and, which SSL keys and certificates exist.

You must log in as the root user to use this command.

#### Related Topic

[Implementing SSL Support in the MWTM, page 2-22](#)

## mwtm start

### Server Only

#### Command Description

Starts all MWTM servers on the local host.

You must log in as the root user or superuser to use this command.



#### Note

---

If the database has an exception during start up, the server will fail to start.

---

#### Related Topic

[Starting the MWTM Server, page 4-1](#)

## mwtm start client

### Server and all Clients

#### Full Syntax

**mwtm start client** [*hostname*]

#### Command Description

Starts an MWTM client on the specified host. If you did not specify a hostname, starts an MWTM client on the default host, as specified during installation. See [Connecting to a New Server, page 5-43](#) for information about determining the default host.

If you log in to a remote workstation through Telnet or SSH, you must set the DISPLAY variable to your local display, or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually (see [Setting the DISPLAY Variable for Solaris or Linux Clients, page 4-3](#)).

This command has the same function as the **mwtm client** command.

## mwtm start jsp

### Server Only

#### Command Description

Starts the MWTM JSP Server on the local host.

You must log in as the root user or superuser to use this command.

## mwtm start pm

### Server Only

#### Command Description

Starts the MWTM Application Server and all managed processes on the local host.

You must log in as the root user or superuser to use this command.

## mwtm start web

### Server Only

#### Command Description

Starts the MWTM web server on the local host.

You must log in as the root user or superuser to use this command.

## mwtm status

### Server Only

#### Command Description

Displays the status of all MWTM servers on the local host.

#### Related Topic

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm stop

### Server Only

#### Command Description

Stops all MWTM servers on the local host.

You must log in as the root user or superuser to use this command.

## mwtm stopclients

### Server and Solaris or Linux Clients Only

#### Command Description

Stops all MWTM clients, including all GTT clients and Event Editors, on the local host.

You must log in as the root user (not as a superuser) to use this command.

## mwtm stop jsp

### Server Only

#### Command Description

Stops the MWTM JSP Server on the local host.

You must log in as the root user or superuser to use this command.

## mwtm stop pm

### Server Only

#### Command Description

Stops the MWTM Application Server and all managed processes on the local host.

You must log in as the root user or superuser to use this command.

## mwtm stop web

### Server Only

#### Command Description

Stops the MWTM web server on the local host.

You must log in as the root user or superuser to use this command.

## mwtm superuser

### Server Only

#### Full Syntax

**mwtm superuser** *[username]*

**Command Description**

Allows the specified user to perform most functions that otherwise require the user to log in as the root user. (The root user can still perform those functions, too.) The specified user account must exist in the local */etc/passwd* file. You cannot specify a user that is defined in a distributed Network Information Services (NIS) system.

**Note**

As a superuser, you can adversely affect your operating environment if you lack a sufficient understanding of the commands that you use. If you are a relatively inexperienced UNIX user, Cisco recommends that you limit your activities as a superuser to the tasks in this document.

For a complete list of the MWTM commands that a superuser cannot use, as well as other superuser considerations, see [Specifying a Super User \(Server Only\)](#), page 2-20.

You must log in as the root user (not as a superuser) to use this command.

## mwtm syncusers

**Server Only****Command Description**

If you enable MWTM User-Based Access and you set **mwtm authtype** to **solaris**, synchronizes local MWTM passwords with Solaris.

You must log in as the root user (not as a superuser) to use this command.

**Related Topic**

[Manually Synchronizing Local MWTM Passwords \(Server Only\)](#), page 2-17

## mwtm tac

**Server Only****Command Description**

Collects important troubleshooting information for the Cisco Technical Assistance Center and writes the information to the */opt/CSCOsgm/tmp/cisco\_mwtm\_tshoot.log* file.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Appendix D, “Troubleshooting the MWTM and the Network”](#)

## mwtm termproxy

### Server Only

### Full Syntax

**mwtm termproxy** [**disable** | **enable** | **status**]

### Command Description

Manages a terminal proxy that resides on a server and forwards terminal requests from clients to nodes that are accessible only from that server. You use a terminal proxy to enable remote clients on desktop networks to connect to nodes that otherwise would be unreachable. You can use these options with this command:

- **disable**—Disables MWTM proxy support. This is the default setting.
- **enable**—Enables the MWTM to use a proxy and prompts you to restart the MWTM server. When you restart the server, the MWTM automatically starts the proxy process.
- **status**—Indicates whether MWTM proxy support is currently enabled or disabled.

You must log in as the root user or superuser to use this command.

### Related Topic

[Enabling the Terminal Server Proxy Service, page 3-11](#)

## mwtm trapaccess

### Server Only

### Full Syntax

**mwtm trapaccess** [**add** [*ip-addr*] | **clear** | **edit** | **list** | **rem** [*ip-addr*] | **sample**]

### Command Description

You use this command to create and manage a list of IP addresses that can send traps to the MWTM server.

The list of allowed IP addresses resides in the *trapaccess.conf* file. By default, when you first install the MWTM, the *trapaccess.conf* file does not exist and the MWTM allows all IP addresses to send traps to the MWTM server. To create the *trapaccess.conf* file and work with the list of allowed client IP addresses, specify one of these keywords:

- **add**—Add the specified IP address to the *trapaccess.conf* file. If the file does not already exist, this command creates the file containing the first entry.
- **clear**—Remove all IP addresses from the *trapaccess.conf* file and allow traps from any MWTM client IP address.
- **edit**—Open and edit the *trapaccess.conf* file directly. If the *trapaccess.conf* file does not already exist, this command creates an empty file.
- **list**—List all IP addresses currently in the *trapaccess.conf* file. If no IP addresses appear (that is, the list is empty), the system allows traps from any MWTM IP address.

- **rem**—Removes the specified IP address from the *trapaccess.conf* file.
- **sample**—Prints out a sample *trapaccess.conf* file.

Any changes that you make take effect when you restart the MWTM server.

For more information about using this command, see [Limiting Traps by IP Address, page 3-9](#).

You must log in as the root user or superuser to use this command.

## mwtm trapratelimit count

### Server Only

This option configures the trap limiting count for nodes or the interval at which nodes are checked for a trap storm.

By default, a node generating 2,000 or more traps (limiting count) in the last 30 minutes (interval) is considered to generate too many traps.

MWTM raises a NodeTrapRate status alarm and stops trap processing for this node. If the node no longer experiences a trap storm in the next cycle (limiting interval), MWTM will automatically reset the ProcessTrap flag and begin processing traps again.

You must log in as the root user or superuser to use this command.

## mwtm trapratelimit interval

### Server Only

This option configures the trap limiting count for nodes or the interval at which nodes are checked for a trap storm.

By default, a node generating 2,000 or more traps (limiting count) in the last 30 mins (interval) is considered to generate too many traps.

MWTM raises a NodeTrapRate status alarm and stops trap processing for this node. If the node no longer experiences a trap storm in the next cycle (limiting interval), MWTM will automatically reset the ProcessTrap flag and begin processing traps again.

You must log in as the root user or superuser to use this command.

## mwtm trapsetup

### Server Only

#### Full Syntax

**mwtm trapsetup [disable]**

#### Command Description

Stops the MWTM server, configures the MWTM to receive SNMP traps (or prevents the MWTM from receiving traps), then restarts the MWTM server.

When you select an SNMP trap port number for the MWTM server, ensure that your ITPs use the same SNMP trap port number. See the description of the **snmp-server host** command in the “ITP Requirements” section of the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for more information.

To prevent the MWTM from receiving traps, enter the **mwtm trapsetup disable** command. The MWTM restarts the MWTM server.

You must log in as the root user (not as a superuser) to use this command.

#### Related Topic

- [Chapter 2, “Configuring Security”](#)
- [Enabling SNMP Traps, page 3-7](#)

## mwtm trapstatus

### Server Only

#### Command Description

Displays the current trap reception configuration for the MWTM, including:

- Whether you enabled or disabled receiving traps.
- On which UDP port the MWTM trap receiver listens.

#### Related Topic

[Enabling SNMP Traps, page 3-7](#)

## mwtm tshootlog

### Server Only

#### Full Syntax

**mwtm tshootlog {enable | disable | status}**

#### Command Description

The MWTM can record all output from troubleshooting commands into a log file. To:

- Record all troubleshooting output to a log file, specify **enable**.
- Stop the MWTM from recording all troubleshooting output to a log file, specify **disable**.
- View the status of this command, specify **status**.

The default path for the troubleshooting log file is `/opt/CSCOs/gm/logs/troubleshooting`. If you installed the MWTM in a directory other than `/opt`, then the troubleshooting log file resides in that directory.

#### Related Topic

[Appendix D, “Troubleshooting the MWTM and the Network”](#)

## mwtm uninstall

### Server and Solaris or Linux Clients Only

#### Command Description

Uninstalls the MWTM.

You must log in as the root user (not as a superuser) to use this command.

## mwtm unknownage

### Server Only

#### Full Syntax

**mwtm unknownage** [*number-of-days*]

#### Command Description

Sets the maximum number of days to retain **Unknown** objects before deleting them from the MWTM database.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 7 days. Setting this value to 0 days means that, after one hour, the system deletes **Unknown**.

You must log in as the root user or superuser to use this command.

## mwtm updateuser

### Server Only

#### Full Syntax

**mwtm updateuser** [*username*]

#### Command Description

If you enable MWTM User-Based Access, changes the authentication level for the specified user. Valid levels are:

- **1**—Basic User.
- **2**—Power User.
- **3**—Network Operator.
- **4**—Network Administrator.
- **5**—System Administrator.

If you set **mwtm authtype** to **local**, you also use this command to change the user's password. When setting the password, follow the rules and considerations in [Creating Secure Passwords, page 2-7](#).

See [Enabling and Changing Users and Passwords \(Server Only\), page 2-14](#) for more information on authentication levels and the use of this command.



You must log in as the root user or superuser to use this command.

**Note**

If you have enabled Solaris authentication, you must log in as the root user, not a superuser, to use this command (see [Configuring User Access, page 2-1](#)).

## mwtm useraccess

### Server Only

### Full Syntax

**mwtm useraccess** [**disable** | **enable**]

### Command Description

Enables or disables MWTM User-Based Access. User-Based Access provides multilevel password-protected access to MWTM features. Each user can have a unique user name and password. You can also assign each user to one of five levels of access, which control the list of MWTM features accessible by that user.

**Note**

You must enable MWTM User-Based Access to use the associated MWTM security commands (see [Configuring User Access, page 2-1](#)).

The **mwtm useraccess** command goes through three stages, checking the status of:

1. **mwtm useraccess**—Enabled or disabled.
2. **mwtm authtype**—If you have not already set the **mwtm** authentication type, you must do so now.
3. **mwtm adduser**—If you have already assigned users, the MWTM asks if you want to use the same user database, or create a new one. If you have not assigned users, you must do so now.

You must log in as the root user or superuser to use this command.

### Related Topic

[Configuring User Access, page 2-1](#)

## mwtm userpass

### Server Only

### Full Syntax

**mwtm userpass** [*username*]

### Command Description

If you enable MWTM User-Based Access and **mwtm authtype** is set to **local**, changes the specified user's MWTM security authentication password.

If the MWTM or a superuser automatically disables the user's authentication, this command re-enables the user's authentication with a new password.

If **mwtm authtype** is set to **solaris**, you cannot use this command; instead, you must manage passwords on the external authentication servers.

You must log in as the root user to use this command.

**Related Topic**

[Enabling and Changing Users and Passwords \(Server Only\)](#), page 2-14

## mwtm version

**Server and Solaris or Linux Clients Only****Command Description**

Displays version information for MWTM servers and clients on the local host.

**Related Topic**

[Chapter 11, “Accessing Data from the Web Interface”](#)

## mwtm viewlog

**Server Only****Command Description**

Uses PAGER to display the contents of the system message log. To:

- Save the current contents of the log, clear the log, and restart the server, enter **mwtm viewlog clear**.
- Display the contents of the log in reverse order, with the most recent messages at the beginning of the log, enter **mwtm msglog -r**.

This command has the same function as the **mwtm msglog** command.

You must log in as the root user or superuser to use this command.

## mwtm wall

**Server Only****Full Syntax**

**mwtm wall** *message\_string*

**Command Description**

Sends a message to all clients that are connected to the server. For example:

**./mwtm wall Server going down at 9:00 pm tonight.**

sends this message:

**Server going down at 9:00 pm tonight.**

The MWTM ignores quotation marks (""") in *message\_string*. To include quotation marks ("""), use the escape character (\) in combination with quotation marks ("""). For example:

**`./mwtm wall` Example of the `\”mwtm wall\”` command.**

sends this message:

**Example of the “mwtm wall” command.**

You must log in as the root user or superuser to use this command.

## mwtm webaccesslog

### Server Only

### Full Syntax

**`mwtm webaccesslog [clear | -r]`**

### Command Description

Uses PAGER to display the MWTM system web access log file for the server to which you connect and which is currently running the MWTM server. The system web access log lists all MWTM system web access messages that it logged for the MWTM server. This method provides an audit trail of all access to the MWTM server via the web interface. To:

- Clear the log and restart the server, enter **`mwtm webaccesslog clear`**.
- Display the contents of the log in reverse order, with the most recent web access messages at the beginning of the log, enter **`mwtm webaccesslog -r`**.

You must log in as the root user or superuser to use this command.

## mwtm weberrorlog

### Server Only

### Full Syntax

**`mwtm weberrorlog [clear | -r]`**

### Command Description

Uses PAGER to display the MWTM web server error log file for the server to which you connect, and which is currently running the MWTM server. The web server error log lists all MWTM web error messages that it logged for the MWTM web server. To:

- Clear the log and restart the server, enter **`mwtm weberrorlog clear`**.
- Display the contents of the log in reverse order, with the most recent web error messages at the beginning of the log, enter **`mwtm weberrorlog -r`**.

You must log in as the root user or superuser to use this command.

## mwtm weblogupdate

### Server Only

### Full Syntax

**mwtm weblogupdate** [*interval* | **disable**]

### Command Description

Controls how often, in seconds, the MWTM updates certain web output.

When you enter this command, the MWTM displays the current interval. You can then change that value or leave it. The valid range is 1 second to an unlimited number of seconds. The default value is 300 seconds (5 minutes).

To disable the update interval, enter the **mwtm weblogupdate disable** command. This option reduces the CPU usage on the server and client.

You must log in as the root user or superuser to use this command.

## mwtm webnames

### Server Only

### Full Syntax

**mwtm webnames** [**display** | **real**]

### Command Description

Specifies whether the MWTM should show real node names or display names in web pages:

- **real**—Displays the real DNS names of nodes in web pages, as discovered by the MWTM.
- **display**—Shows display names in web pages. Display names are new names that you specify for nodes. This is the default setting. For more information about display names, see [Editing Properties, page 6-33](#).

You must log in as the root user or superuser to use this command.

## mwtm webport

### Server Only

### Full Syntax

**mwtm webport** [*port-number*]

### Command Description

Sets a new port number for the web server, where *port-number* is the new, numeric port number. The MWTM verifies that the new port number is not already in use.

The new port number must contain only numbers. If you enter a port number that contains nonnumeric characters, such as **mwtm13**, the MWTM displays an error message and returns to the command prompt without changing the port number.

You must log in as the root user (not as a superuser) to use this command.

## mwtm webutil

### Server Only

#### Full Syntax

**mwtm webutil** [percent | erlangs]

#### Command Description

Specifies whether the MWTM should display send and receive utilization for linksets and links as percentages or in Erlangs (E), in web pages:

- **percent**—The MWTM displays utilization as a percentage (%). This is the default setting.
- **erlangs**—The MWTM displays utilization in Erlangs (E).

You must log in as the root user or superuser to use this command.

#### Related Topic

- [Chapter 11, “Accessing Data from the Web Interface”](#)
- [Chapter 12, “Managing Reports”](#)
- [Locating Stored ITP Reports, page 12-63](#)

## mwtm who

### Server Only

#### Command Description

Displays a list of all client user names and processes connected to the server.

## mwtm xtermopath

### Server or Solaris or Linux Clients Only

#### Command Description

Specifies the path to the **xterm** application to use for xterm sessions on the MWTM client, as well as any special parameters to pass to the xterm application. The default path is */usr/openwin/bin/xterm*.

If one of the special parameters that you pass to the **xterm** application is a title, the title can contain hyphens (-) and underscores (\_), but no spaces.

You must log in as the root user (not as a superuser) to use this command.

# ITP-Only Commands

ITP-only commands include:

- [mwtm accstats](#), page B-87
- [mwtm archivedir](#), page B-88
- [mwtm atblclient](#), page B-89
- [mwtm atbldir](#), page B-90
- [mwtm autosynconfig](#), page B-91
- [mwtm chartwindow](#), page B-91
- [mwtm checkgtt](#), page B-91
- [mwtm checkgtt](#), page B-91
- [mwtm checkmlr](#), page B-92
- [mwtm checkroute](#), page B-92
- [mwtm countas](#), page B-92
- [mwtm countasp](#), page B-92
- [mwtm countaspa](#), page B-93
- [mwtm countlinks](#), page B-93
- [mwtm countlinksets](#), page B-93
- [mwtm countsgrp](#), page B-93
- [mwtm countsps](#), page B-93
- [mwtm deletearchive](#), page B-94
- [mwtm deployarchive](#), page B-94
- [mwtm deploycomments](#), page B-95
- [mwtm evreps clean](#), page B-95
- [mwtm evreps cleancustom](#), page B-95
- [mwtm evreps diskcheck](#), page B-95
- [mwtm evreps enable](#), page B-96
- [mwtm evreps hourlyage](#), page B-96
- [mwtm evreps mtp](#), page B-97
- [mwtm evreps status](#), page B-97
- [mwtm evreps timer](#), page B-97
- [mwtm gttclient](#), page B-98
- [mwtm gttldir](#), page B-98
- [mwtm gttstats](#), page B-100
- [mwtm linkstats](#), page B-101
- [mwtm listarchive](#), page B-103
- [mwtm listgtt](#), page B-103
- [mwtm listgtt](#), page B-103

- [mwtm listhistory](#), page B-104
- [mwtm listmlr](#), page B-104
- [mwtm listroute](#), page B-104
- [mwtm mlrstats](#), page B-105
- [mwtm mtpevents](#), page B-106
- [mwtm pcformat](#), page B-107
- [mwtm pclist](#), page B-108
- [mwtm pushgtt](#), page B-108
- [mwtm pushgtt](#), page B-108
- [mwtm pushmlr](#), page B-109
- [mwtm pushroute](#), page B-110
- [mwtm q752stats](#), page B-110
- [mwtm repcustage](#), page B-112
- [mwtm repdir](#), page B-112
- [mwtm replog](#), page B-113
- [mwtm routedir](#), page B-114
- [mwtm routetabledefs](#), page B-115
- [mwtm start atblclient](#), page B-115
- [mwtm start gttclient](#), page B-116
- [mwtm statreps acct](#), page B-117
- [mwtm statreps clean](#), page B-117
- [mwtm statreps cleancustom](#), page B-118
- [mwtm statreps custage](#), page B-118
- [mwtm statreps dailyage](#), page B-119
- [mwtm statreps diskcheck](#), page B-119
- [mwtm statreps enable](#), page B-120
- [mwtm statreps export](#), page B-120
- [mwtm statreps gtt](#), page B-121
- [mwtm statreps hourlyage](#), page B-121
- [mwtm statreps iplinks](#), page B-122
- [mwtm statreps link](#), page B-122
- [mwtm statreps maxcsvrows](#), page B-123
- [mwtm statreps mlr](#), page B-123
- [mwtm statreps msu](#), page B-124
- [mwtm statreps nullcaps](#), page B-125
- [mwtm statreps q752](#), page B-125
- [mwtm statreps servratio](#), page B-126
- [mwtm statreps status](#), page B-126



- [mwtm statreps timemode](#), page B-127
- [mwtm statreps timer](#), page B-127
- [mwtm statreps xua](#), page B-128
- [mwtm webutil](#), page B-84
- [mwtm xuastats](#), page B-129

## mwtm accstats

### Server Only

### Full Syntax

**mwtm accstats** [*nodes* [*linksets* [*filter*]] [*idtag*]] [*sortopts*] [**quiet**]

### Command Description

Generates MWTM accounting statistics reports. To:

- Include or exclude specific objects in the reports, use the *nodes* argument. To include:
  - All nodes, specify **all**.
  - A single node or signaling point, specify a single node name, or node name and signaling-point name, as the *nodes* argument. The node name must exactly match the node name that the MWTM discovered, including the domain name; for example:

```
mwtm-75-59a.cisco.com
```

To specify a node name and signaling point:

```
mwtm-75-59a.cisco.com;net0
```

- Linksets, specify a filename with a list of linksets:
 

```
mwtm-75-96a.cisco.com;net0:7291p_to_7591a0
```
- A filter, specify a filename with a list of filters in the format *dpc:opc*:
 

```
1.2.0:1.17.0
```
- Or exclude objects based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This is also the default setting for this command; you only need to specify **default** if you also want to specify an *idtag*, *sortopts*, or **quiet**.
- A group of nodes or signaling points other than the one specified in the *nodes.include* file, create a file that contains the list of nodes and signaling points to include and specify the full path and name of the file as the *nodes* argument.



**Note** For more details on including and excluding objects, see [Including or Excluding Specified Objects in ITP Reports](#), page 12-4.

If you specify *nodes*, you can also specify an *idtag* to identify the reports. The *idtag* can be any meaningful character string, but it cannot contain any spaces. The default value for *idtag* is the process ID of the **mwtm accstats** command.

- Specify the sort order for the reports, specify one of these keywords for the *sortopts* argument:
  - sdp**—Sort based on the destination point code (DPC) of the node, in ascending order.
  - sno**—Sort based on the node name, in ascending order.
  - sop**—Sort based on the originating point code (OPC) of the node, in ascending order.
  - srb**—Sort based on the number of bytes received, in descending order.
  - srm**—Sort based on the number of MTP3 message signal units (MSUs) received, in descending order.
  - ssb**—Sort based on the number of bytes sent, in descending order.
  - ssi**—Sort numerically based on service indicator (SI), in ascending order.
  - ssm**—Sort based on the number of MTP3 MSUs sent, in descending order.
- Disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. The MWTM generates the report in export format, which you view by using the MWTM web interface.

Before entering this command, you must enable the MWTM to generate accounting statistics reports. See the description of the **mwtm statreps [acct | noacct]** command for more information.

The first time you use the **mwtm acctstats** command to generate a report, you must enter the command at least twice. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful accounting statistics and, if the collected data appears valid, begins generating the report.

Thereafter, you need only to enter this command once to generate the report.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Customizing ITP Report Preferences, page 12-65](#)

## mwtm archivedir

### Server Only

### Full Syntax

**mwtm archivedir** [*directory*]

### Command Description



#### Note

You must stop the MWTM server before performing this command. The system prompts you whether to continue.

Sets the Version Control System (VCS) repository directory, the directory in which the MWTM stores archived files.

The default VCS repository directory resides in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the directory is */opt/CSCOs/gm/vcs-repository*.
- A different directory, then the directory resides in that directory.

Use this command if you want to use a different directory; for example, a Network File System location on another server.

- This command copies all files in the current directory to the new directory. If you do not log in as the superuser and do not own the new directory, you might not be able to copy the files. In that case, you must specify a directory that you own or you must log in as the root user. Do not set the new directory to:
  - Any of these: */usr*, */var*, */opt*, or */tmp*.
  - The same directory in which you are storing message log files (**mwtm msglogdir**), report files (**mwtm repdir**), route table files (**mwtm routedir**), GTT files (**mwtm gttidir**), or address table files (**mwtm atbldir**).

You must log in as the root user or superuser to use this command.

**Note**

If you are setting up a new repository directory on a Network File System location on another (remote) server, ensure that the server allows read-write access to the user account that you use to run the MWTM and run this command as a superuser.

## mwtm atblclient

### Solaris or Linux Clients Only

#### Full Syntax

**mwtm atblclient** [*hostname*]

#### Command Description

Starts an MWTM Address Table Editor client on the specified host. If you do not specify a hostname, starts an MWTM Address Table Editor client on the default host, as specified during installation. See [Connecting to a New Server, page 5-43](#) for information about determining the default host.

For more information about the MWTM Address Table Editor, see [Chapter 15, “Editing ITP MLR Address Table Files.”](#)

If you log in to a remote workstation through Telnet, you must set the DISPLAY variable to your local display or you cannot use this command. If the system does not automatically set the DISPLAY variable, you must set it manually (see [Setting the DISPLAY Variable for Solaris or Linux Clients, page 4-3](#)).

## mwtm atbldir

### Server Only

### Full Syntax

**mwtm atbldir** [*directory*]

### Command Description



#### Note

You must stop the MWTM server before performing this command. The system then prompts you whether to continue.

Sets the address-table staging directory, the directory in which the MWTM stores address table files. For more information about address table files, see [Chapter 15, “Editing ITP MLR Address Table Files.”](#)

The default address table staging directory resides in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the directory is */opt/CSCOsgm/atbl*.
- A different directory, then the directory resides in that directory.

Use this command if you want to use a different directory to stage address tables, such as */ftpboot*, or such as a Network File System location on another server, used as the TFTP server for server configuration files for ITPs in the network.

This command copies all files in the current directory to the new directory. If you are not logged in as the superuser and do not own the new directory, the MWTM provides this prompt:

```
Can't create directory!! Address Table Staging Directory not changed!!
```

```
Directory could be located on a remote NFS server.
Manually create directory and try again.
Set permissions using chmod 777.
```

You must specify a directory that you own, or you must log in as the root user. Do not set the new directory to:

- Any of these: */usr*, */var*, */opt*, or */tmp*.
- The same directory in which you are storing message log files (**mwtm msglogdir**), report files (**mwtm repdir**), route table files (**mwtm routedir**), or GTT files (**mwtm gttdir**).

When you enter this command, the MWTM also prompts you to enable TFTP file transfer for the address table staging directory and prompts you for the TFTP path for the directory, **tftp://hostname/path**, where:

- *hostname* is the name or IP address of the host on which the address-table staging directory resides.

If you enter a DNS name (such as **mwm-jumbo**) instead of an IP address (such as **172.18.12.10**), then the ITP must be able to resolve the DNS name; otherwise, when you try to deploy a file, the MWTM issues an appropriate error message and does not deploy the file.

To enable the ITP to resolve DNS names, enter the **ip domain-lookup** command on the ITP. For more information about this command, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*, Release 12.3 or later.

- *path* is the path to the address table staging directory.

After you change the directory or enable TFTP file transfer for the directory, the MWTM asks if you want to restart the MWTM server. The new directory and TFTP setting take effect when you restart the MWTM server.

You must log in as the root user or superuser to use this command.

**Note**

If you are setting up a new address table staging directory on a Network File System location on another (remote) server, ensure that the server allows read-write access to the user account through which the MWTM is running and run this command as a superuser.

## mwtm autosynconfig

**Server Only****Full Syntax**

**mwtm autosynconfig** [enable | disable | status]

**Command Description**

Manages **auto sync** configuration settings to automatically save the IOS configuration changes.

## mwtm chartwindow

**Server Only****Full Syntax**

**mwtm chartwindow** [mins | clear]

**Command Description**

Specifies the maximum amount of data appearing (in minutes) for real-time ITP charts.

For example, if you set this command to 20 minutes, the charts are refreshed every 20 minutes to show the latest data. The valid range is between 5 and 120 minutes, and the default setting is 15 minutes.

To return to the default setting, enter the **mwtm chartwindow clear** command.

You must log in as the root user or superuser to use this command.

## mwtm checkgtt

**Server Only****Full Syntax**

**mwtm checkgtt** [-l logfilename] filename signalingpointname

**Command Description**

Checks the semantics and syntax of the specified GTT file on the specified signaling point. To write detailed syntax- and semantics-checking results to a file, specify **-l** and the name of the file.

You must log in as the root user or superuser to use this command.

## mwtm checkmlr

### Server Only

### Full Syntax

**mwtm checkmlr** [-l *logfile*] *filename* *signalingpointname*

### Command Description

Checks the semantics and syntax of the specified MLR address table on the specified signaling point. To write detailed syntax- and semantics-checking results to a file, specify -l and the name of the file.

You must log in as the root user or superuser to use this command.

## mwtm checkroute

### Server Only

### Full Syntax

**mwtm checkroute** [-l *logfile*] *filename* *signalingpointname*

### Command Description

Checks the semantics and syntax of the specified route table file on the specified signaling point. To write detailed syntax- and semantics-checking results to a file, specify -l and the name of the file.

You must log in as the root user or superuser to use this command.

## mwtm countas

### Server Only

### Command Description

Displays a count of application servers in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm countasp

### Server Only

### Command Description

Displays a count of application server processes in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm countaspa

### Server Only

#### Command Description

Displays a count of application server process applications in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm countlinks

### Server Only

#### Command Description

Displays a count of links in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm countlinksets

### Server Only

#### Command Description

Displays a count of linksets in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm countsgmp

### Server Only

#### Command Description

Displays a count of signaling gateway-mated pairs in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm countsp

### Server Only

#### Command Description

Displays a count of signaling points in the current MWTM database.

You must log in as the root user or superuser to use this command.

## mwtm deletearchive

### Server Only

#### Full Syntax

**mwtm deletearchive** *{-s signaling-point-name} {-t type} [-a address-table-name]*

#### Command Description

Deletes a file from the archive.

- To delete an archived file, specify **-s** and the name of the signaling point, and specify **-t** and the type, which can be one of these:
  - gtt**
  - route**
  - mlr**



**Note** If you specify the *type* as **mlr**, you must also specify **-a** and the name of the address table.

You must log in as the root user or superuser to use this command.

## mwtm deployarchive

### Server Only

#### Full Syntax

**mwtm deployarchive** *{-s signaling point name of source configuration} {-t type} [-a address table name] [-r revision number of file] [-c archive comment for deploy]*

#### Command Description

Allows you to deploy an archived file to a specified signaling point. To:

- Deploy an archived file, specify **-s** and the name of the source configuration signaling point and specify **-t** and the type, which can be one of these:
  - gtt**
  - route**
  - mlr**



**Note** If you specify the *type* as **mlr**, you must also specify **-a** and the name of the address table.

- Deploy a specific revision number of the archive file, specify **-r** and the revision number. If the revision is not specified, the current revision is deployed.
- Provide archive comments during deployment, specify **-c** and add your comments.

Once you have entered the command, you will receive a prompt to enter the destination signaling-point name.

You must log in as the root user or superuser to use this command.



## mwtm deploycomments

### Server Only

#### Full Syntax

**mwtm deploycomments** { **required** | **optional** | **status** }

#### Command Description

Allows you to require or make optional user comments during deployment. To:

- Prompt the user for comments during file archiving by using the wizard, specify **required**.
- Skip the prompt for comments during file archiving by using the wizard, specify **optional**. You can still specify comments by using CLI commands, such as **mwtm pushgtt**, **mwtm pushmlr**, and **mwtm pushroute**.
- Show the current settings on the command line, specify **status**.

You must log in as the root user or superuser to use this command.

## mwtm evreps clean

### Server Only

#### Command Description

Removes all data from MWTM network event reports, restoring the reports to an unchanged state.

You must log in as the root user or superuser to use this command.

## mwtm evreps cleancustom

### Server Only

#### Full Syntax

**mwtm evreps cleancustom** [*tag*]

#### Command Description

Removes all data from one or more MWTM custom event reports, restoring the reports to an unchanged state. To clean:

- All custom reports, enter **mwtm evreps cleancustom**.
- A single custom report, enter **mwtm evreps cleancustom tag**, where *tag* is the ID tag of the custom report that you want to clean.

You must log in as the root user or superuser to use this command.

## mwtm evreps diskcheck

#### Full Syntax

**mwtm evreps** [ **diskcheck** | **nodiskcheck** ]

**Command Description**

Specifies whether the MWTM should verify that a disk has at least 10 MB of space remaining before generating network event reports:

- **diskcheck**—Verify the disk space. This is the default setting.
- **nodiskcheck**—Do not verify the disk space.

If your system does not return the necessary amount of free space in a correct format that the MWTM can parse, use this command to disable checking and to allow reporting to continue.

See [Chapter 12, “Managing Reports”](#) for more information on the output of this command.

You must log in as the root user or superuser to use this command.

## mwtm evreps enable

**Server Only****Full Syntax**

**mwtm evreps** [**disable** | **enable**]

**Command Description**

Enables the MWTM to generate event reports:

- **enable**—Generate network event reports. This is the default setting.
- **disable**—Do not generate network event reports.

The **mwtm evreps** command enables or disables the MWTM event reporting feature. To enable a specific type of event reporting, you must also enable that report type.

**Note**

In this release, the only event reports that the MWTM can generate are MTP3 events (see [mwtm evreps mtp](#), page B-97). To enable the MWTM event reporting feature, enter **mwtm evreps enable**. Then, to enable MTP3 event reporting, enter **mwtm evreps mtp**. To manually generate an MTP report from the command line, see [mwtm mtpevents](#), page B-106.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Chapter 12, “Managing Reports”](#)

## mwtm evreps hourlyage

**Server Only****Full Syntax**

**mwtm evreps hourlyage** [*number-of-days*]

**Command Description**

Maximum number of days the MWTM should archive hourly network event reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 31 days.

You must log in as the root user or superuser to use this command.

## mwtm evreps mtp

### Server Only

#### Full Syntax

**mwtm evreps** [**mtp** | **nomtp**]

#### Command Description

Specifies whether the MWTM should generate MTP3 event reports:

- **mtp**—Generate MTP3 event reports.
- **nomtp**—Do not generate MTP3 event reports. This is the default setting.



#### Note

The default setting for MTP3 event reporting is disabled. To enable MTP3 event reporting, first enter **mwtm evreps enable** (see [mwtm evreps enable](#), page B-96). Then enter **mwtm evreps mtp**.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Chapter 12, “Managing Reports”](#)

## mwtm evreps status

### Server Only

#### Command Description

Displays the current status of all MWTM network event report parameters. You set these parameters by using the other **mwtm evreps** commands, such as:

- **mwtm evreps** [**disable** | **enable**]
- **mwtm evreps** [**diskcheck** | **nodiskcheck**]

You must log in as the root user or superuser to use this command.

## mwtm evreps timer

### Server Only

#### Command Description

Displays the timer file for MWTM network event reports. The timer file is useful for identifying how much time the MWTM spends gathering report data and generating reports.

You must log in as the root user or superuser to use this command.

## mwtm gttclient

### Solaris or Linux Clients Only

#### Full Syntax

**mwtm gttclient** [*hostname*]

#### Command Description

Starts an MWTM GTT client on the specified host. If no hostname is specified, starts an MWTM GTT client on the default host, as specified during installation. See [Connecting to a New Server, page 5-43](#) for information about determining the default host.

For more information about the MWTM GTT client, see [Chapter 14, “Editing an ITP Global Title Translation Table.”](#)

If you access a remote workstation through Telnet, you must set the DISPLAY variable to your local display or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually (see [Setting the DISPLAY Variable for Solaris or Linux Clients, page 4-3](#)).

## mwtm gttmdir

### Server Only

#### Full Syntax

**mwtm gttmdir** [*directory*]

#### Command Description



#### Note

You must stop the MWTM server before performing this command. The system prompts you whether to continue.

Sets the GTT staging directory, the directory in which the MWTM stores GTT files and enables Trivial File Transfer Protocol (TFTP) file transfer for the directory. See [Chapter 14, “Editing an ITP Global Title Translation Table”](#) for information about GTT files.

The default GTT staging directory resides in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the directory is */opt/CSCOsgm/gtt*.
- A different directory, then the directory resides in that directory.

Use this command if you want to use a different GTT staging directory, such as */tftpboot* or the Network File System location on another server, which is used as the TFTP server for server configuration files for ITPs in the network.

This command copies all files in the current directory to the new directory. If you are not logged in as the superuser and do not own the new directory, the MWTM provides this prompt:

```
Can't create directory!! GTT Directory not changed!!
```

```
Directory could be located on a remote NFS server.
Manually create directory and try again.
Set permissions using chmod 777.
```

You must specify a directory that you own, or you must log in as the root user. Do not set the new directory to any of these: */usr*, */var*, */opt*, or */tmp*.

Do not set the new directory to the same directory in which you are storing:

- Message log files (**mwtm msglogdir**)
- Report files (**mwtm repdir**)
- Route table files (**mwtm routedir**)
- Address table files (**mwtm atbldir**)

When you enter this command, the MWTM also prompts you to enable TFTP file transfer for the GTT staging directory and prompts you for the TFTP path for the directory, **tftp://hostname/path**, where:

- *hostname* is the name or IP address of the host on which the GTT staging directory resides.  
  
If you enter a DNS name (such as **mwm-jumbo**) instead of an IP address (such as **172.18.12.10**), then the ITP must be able to resolve the DNS name; otherwise, when you try to deploy a file, the MWTM issues an appropriate error message and does not deploy the file.  
  
To enable the ITP to resolve DNS names, enter the **ip domain-lookup** command on the ITP. For more information about this command, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*, Release 12.3 or later.
- *path* is the path to the GTT staging directory.

After you change the directory or enable TFTP file transfer for the directory, the MWTM asks if you want to restart the MWTM server. The new directory and TFTP setting take effect when you restart the MWTM server.

You must log in as the root user or superuser to use this command.

**Note**

If you are setting up a new GTT staging directory on a Network File System location on another (remote) server, ensure that the server allows read-write access to the user account through which the MWTM is running and run this command as a superuser.

## mwtm gttstats

### Server Only

#### Full Syntax

**mwtm gttstats** [*nodes* [*linksets* [*filter*]] [*idtag*]] [*sortopts*] [**quiet**]

#### Command Description

Generates MWTM GTT accounting statistics reports. To:

- Include or exclude specific objects in the reports, use the *nodes* argument. To include:
  - All nodes, specify **all**.  
A single node or signaling point, specify a single node name, or node name and signaling-point name, as the *nodes* argument. The node name must exactly match the node name that the MWTM discovered, including the domain name, and each line must end with a colon (:).  
For example:  
`mwtm-75-59a.cisco.com:`
  - To specify a node name and signaling point, enter:  
`mwtm-75-59a.cisco.com;net0:`
  - Linksets, specify a filename with a list of linksets:  
`mwtm-75-96a.cisco.com;net0:7291p_to_7591a0`
  - A filter, specify a filename with a list of filters in the format:  
`selname:gta:pc`
  - Or exclude objects based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This setting is also the default for this command; you only need to specify **default** if you also want to specify an *idtag*, *sortopts*, or **quiet**.
  - A group of nodes or signaling points other than the one that the *nodes.include* file specifies, create a file that contains the list of nodes and signaling points to include, and specify the full path and name of the file as the *nodes* argument.



**Note** For more details on including and excluding objects, see [Including or Excluding Specified Objects in ITP Reports, page 12-4](#).

If you specify a *nodes*, you can also specify an *idtag* to identify the reports. The *idtag* can be any meaningful character string, but it cannot contain any spaces. The default value for *idtag* is the process ID of the **mwtm gttstats** command.

- Specify the sort order for the reports, specify one of these keywords for the *sortopts* argument:
  - **-sgt**—Sort based on the GTA, in descending order.
  - **-sno**—Sort based on the node name, in ascending order.
  - **-spc**—Sort based on the point code, in ascending order.
  - **-ssn**—Sort based on the selector name, in ascending order.
  - **-sto**—Sort based on the total number of octets translated by GTT, in descending order.

- **-stp**—Sort based on the total number of packets translated by GTT, in descending order. This is the default setting.
- Disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. The MWTM generates the report in export format, which you can view by using the MWTM web interface.

Before entering this command, you must enable the MWTM to generate GTT accounting statistics reports. See the description of the **mwtm statreps [gtt | nogtt]** command for more information.

The first time you use the **mwtm gttstats** command to generate a report, you must enter the command at least twice. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful accounting statistics and, if the collected data appears valid, begins generating the report.

Thereafter, you only need to enter this command once to generate the report.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Customizing ITP Report Preferences, page 12-65](#)

## mwtm linkstats

### Server Only

### Full Syntax

**mwtm linkstats** [*nodes* [*linksets*] [*idtag*]] [*sortopts*] [**quiet**]

### Command Description

Generates MWTM link and linkset statistics summary reports. To include:

- Or exclude specific objects in the reports, use the *nodes* argument. To include:
  - All nodes, specify **all**.
  - A single node or signaling point, specify a single node name, or node name and signaling-point name, as the *nodes* argument. The node name must exactly match the node name that the MWTM discovered, including the domain name, and each line must end with a colon (:).

For example:

```
mwtm-75-59a.cisco.com:
```

A node name and signaling point:

```
mwtm-75-59a.cisco.com;net0:
```

- Linksets, specify a filename with a list of linksets:
 

```
mwtm-75-96a.cisco.com;net0:7291p_to_7591a0
```
- Or exclude objects based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This setting is also the default for this command; you only need to specify **default** if you also want to specify an *idtag*, *sortopts*, or **quiet**.

- A group of nodes or signaling points other than the one specified in the *nodes.include* file, create a file that contains the list of nodes and signaling points to include; and, specify the full path and name of the file as the *nodes* argument.

If you specify *nodes*, you can also specify an *idtag* to identify the reports. The *idtag* can be any meaningful character string, but it cannot contain any spaces. The default value for *idtag* is the process ID of the **mwtm linkstats** command.

- Specify the sort order for the reports, specify one of these keywords for the *sortopts* argument:
  - **-sco**—Sort based on the average Congestion for each link (**Avg Cong %**), in descending order.
  - **-sis**—Sort based on in-service percentage for each link (**InSrv**), in descending order.
  - **-sls**—Sort based on the linkset name, in ascending order.
  - **-srm**—Sort based on the total number of MTP3 MSUs that each link (**Recv MSUs**) receives, in descending order.
  - **-sru**—Sort based on the average Receive Utilization for each link (**Avg Receive Util** or **Avg Receive Erls**), in descending order.
  - **-ssm**—Sort based on the total number of MTP3 MSUs that each link (**Send MSUs**) sends, in descending order.
  - **-ssu**—Sort based on the average Send Utilization for each link (**Avg Send Util** or **Avg Send Erls**), in descending order. This is the default setting.
- Disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. The MWTM generates the report in export format, which you can view by using the MWTM web interface.

Before entering this command, you must enable the MWTM to generate link and linkset statistics summary reports. See the description of the **mwtm statreps [link | nolink]** command for more information.

The first time you use the **mwtm linkstats** command to generate a report, you must enter the command at least three times. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful link and linkset statistics.
- Third entry continues to calculate statistics, calculates long-term averages; and, if the collected data appears valid, begins generating the report.

Thereafter, you only need to enter this command once to generate the report.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Link Reports, page 12-17](#)

[Linkset Reports, page 12-23](#)



## mwtm listarchive

### Server Only

#### Full Syntax

**mwtm listarchive** {**-n** *node name* | **-s** *signaling point name*} {**-t** *type*} [**-a** *address table name*]

#### Command Description

Displays a list of all the files in the Version Control System (VCS) archive or just those of a particular type for a specified node or signaling point. To show a list of files in the VCS of a particular:

- Node, specify **-n** and the node name.
- Signaling point, specify **-s** and the name of the signaling point.
- Type, specify **-t** and the type, which can be one of these:
  - **gtt**
  - **route**
  - **mlr**



**Note** If you specify the *type* as **mlr**, you must also specify **-a** and the name of the address table.

You must log in as the root user or superuser to use this command.

## mwtm listgtt

### Server Only

#### Full Syntax

**mwtm listgtt** [*directory*]

#### Command Description

Lists all current GTT files in the specified directory (*directory* must be a subdirectory of the GTT staging directory). If no directory is specified, lists all current GTT files in the GTT staging directory.

You must log in as the root user or superuser to use this command.

## mwtm listhistory

### Server Only

#### Full Syntax

**mwtm listhistory** {-s *signaling point name*} {-t *type*} [-a *address table name*]

#### Command Description

Displays the revision history for a specified archive file. To show the revision history for a particular:

- Signaling point, specify -s and the name of the signaling point.
- Type of file, specify -t and the type, which can be one of these:
  - gtt
  - route
  - mlr



**Note** If you specify the *type* as **mlr**, you must also specify -a and the name of the address table.

You must log in as the root user or superuser to use this command.

## mwtm listmlr

### Server Only

#### Full Syntax

**mwtm listmlr** [*directory*]

#### Command Description

Lists all current MLR address files in the address table staging directory (for details on setting the address table staging directory, see [mwtm atbldir](#), page B-90.) If a subdirectory is specified, lists all current MLR address files in the specified subdirectory (*directory* must be a subdirectory of the address table staging directory).

You must log in as the root user or superuser to use this command.

## mwtm listroute

### Server Only

#### Full Syntax

**mwtm listroute** [*directory*]

#### Command Description

Lists all current route table files in the specified directory (*directory* must be a subdirectory of the DPC Route staging directory). If no directory is specified, lists all current route table files in the DPC Route staging directory.

You must log in as the root user or superuser to use this command.

## mwtm mlrstats

### Server Only

### Full Syntax

**mwtm mlrstats** [*nodes* [*idtag*]] [*sortopts*] [**quiet**]

### Command Description

Generates MWTM MLR processed, aborts, continues, result invokes, rule matches, subtriggers, and triggers reports. To:

- Include or exclude specific objects in the reports, use the *nodes* argument. To include:
  - All nodes, specify **all**.
  - A single node or signaling point, specify a single node name, or node name and signaling point name, as the *nodes* argument. The node name must exactly match the node name that the MWTM discovered, including the domain name.

For example:

```
mwtm-75-59a.cisco.com
```

To specify a node name and signaling point:

```
mwtm-75-59a.cisco.com;net0
```

- Or exclude objects based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This setting is also the default for this command; you only need to specify **default** if you also want to specify an *idtag*, *sortopts*, or **quiet**.
- A group of nodes or signaling points other than the one specified in the *nodes.include* file, create a file that contains the list of nodes and signaling points to include and specify the full path and name of the file as the *nodes* argument.



**Note** For more details on including and excluding objects, see [Including or Excluding Specified Objects in ITP Reports, page 12-4](#).

If you specify *nodes*, you can also specify an *idtag* to identify the reports. The *idtag* can be any meaningful character string, but it cannot contain any spaces. The default value for *idtag* is the process ID of the **mwtm mlrstats** command.

- Specify the sort order for the reports, specify one of these keywords for the *sortopts* argument:
  - **-sab**—Sort based on the number of MSUs not processed by MLR (**Aborts**), in descending order.
  - **-sal**—Sort based on the number of MSUs of type GSM-MAP AlertSc that MLR (**MAP Alerts**) processed, in descending order.
  - **-sco**—Sort based on the number of MSUs passed back to SCCP that MLR (**Continue**) processed, in descending order.
  - **-smo**—Sort based on the number of MSUs of type GSM-MAP SMS-MO that MLR (**MAP SMS-MOs**) processed, in descending order.

- **-smt**—Sort based on the number of MSUs of type GSM-MAP SMS-MT that MLR (**MAP SMS-MTs**) processed, in descending order.
- **-sno**—Sort based on the node name, in ascending order.
- **-snt**—Sort based on the number of MSUs of type ANSI-41 SMSNotify that MLR (**ANSI-41 SMS-Notifys**) processed, in descending order.
- **-spp**—Sort based on the number of MSUs of type ANSI-41 SMD-PP that MLR (**ANSI-41 SMD-PPs**) processed, in descending order.
- **-sre**—Sort based on the number of MSUs of type ANSI-41 SMSRequest that MLR (**ANSI-41 SMD-Reqs**) processed, in descending order.
- **-sri**—Sort based on the number of MSUs of type GSM-MAP SRI-SM that MLR (**MAP SRI-SMs**) processed, in descending order.
- **-sro**—Sort based on the number of packets that MLR (**Routed**) routed, in descending order.
- Disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. The MWTM generates the report in export format, which you can view by using the MWTM web interface.

If you do not specify the **quiet** keyword (that is, if you view the output on your terminal), the MWTM displays only instance-level statistics (as listed in the description of the *sortopts* argument). To see the full set of trigger-level statistics, you must use the MWTM web interface (see [MLR Reports, page 12-27](#)).

Before entering this command, you must enable the MWTM to generate MLR processed, aborts, continues, result invokes, rule matches, subtriggers, and triggers reports. See the description of the **mwtm statreps [mlr | nomlr]** command for more information.

The first time you use the **mwtm mlrstats** command to generate a report, you must enter the command at least twice. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful accounting statistics and, if the collected data appears valid, begins generating the report.

Thereafter, you only need to enter this command once to generate the report.

See [MLR Reports, page 12-27](#) for more information on MLR reports.

You must log in as the root user or superuser to use this command.

## mwtm mtpevents

### Server Only

### Full Syntax

**mwtm mtpevents** [*nodes* [*idtag*]] [**quiet**]

### Command Description

Generates MWTM MTP3 event reports. To:

- Include or exclude specific objects in the reports, use the *nodes* argument. To include:
  - All nodes, specify **all**.

- A single node or signaling point, specify a single node name, or node name and signaling-point name, as the *nodes* argument. The node name must exactly match the node name that the MWTM discovered, including the domain name.

For example:

```
mwtm-75-59a.cisco.com
```

To specify a node name and signaling point:

```
mwtm-75-59a.cisco.com;net0
```

- Or exclude objects based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This setting is also the default for this command; you only need to specify **default** if you also want to specify an *idtag* or **quiet**.
- A group of nodes or signaling points other than the one that the *nodes.include* file specified, create a file that contains the list of nodes and signaling points to include; and, specify the full path and name of the file as the *nodes* argument.



**Note**

For more details on including and excluding objects, see [Including or Excluding Specified Objects in ITP Reports, page 12-4](#).

If you specify *nodes*, you can also specify an *idtag* to identify the reports. The *idtag* can be any meaningful character string, but it cannot contain any spaces. The default value for *idtag* is the process ID of the **mwtm mtpevents** command.

- Disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. The MWTM generates the report in export format, which you can view by using the MWTM web interface.

The first time you use the **mwtm mtpevents** command to generate a report, you must enter the command at least twice. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful accounting statistics and, if the collected data appears valid, begins generating the report.

Thereafter, you need only enter this command once to generate the report.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Customizing ITP Report Preferences, page 12-65](#)

## mwtm pcformat

**Server Only**

**Full Syntax**

```
mwtm pcformat {edit | list | master | restore}
```

**Command Description**

You use this command to set the point code format for this MWTM server and for all associated MWTM clients to use. You need to set the point code format usually only once, after installation.

You also use this command to configure the MWTM to recognize a single-instance ITP connecting to multiple instances on a multiple-instance ITP. In effect, the MWTM views the multiple networks as a single all-encompassing network.

The point code format configuration is contained in the *PointCodeFormat.xml* file. To work with the file, specify one of these keywords:

- **edit**—Opens the *PointCodeFormat.xml* file for editing.
- **list**—Displays the current contents of the *PointCodeFormat.xml* file.
- **master**—Restores the *PointCodeFormat.xml* file to the default settings.
- **restore**—Restores the *PointCodeFormat.xml* file to the last saved copy.

Any changes that you make take effect when you restart the MWTM server.

The MWTM preserves customized point code formats when you upgrade to a new version or release of the MWTM.

See [Setting the ITP Point Code Format, page 3-5](#) and [Connecting a Single-Instance ITP to a Multiple-Instance ITP, page 3-6](#) for more information about using this command.

You must log in as the root user or superuser to use this command.

## mwtm pclist

**Server Only****Command Description**

Lists all point codes that all nodes that the MWTM detects are currently using.

You must log in as the root user or superuser to use this command.

## mwtm pushggt

**Server Only****Full Syntax**

```
mwtm pushggt [-l logfilename] [-u username] [-p password] [-n enableusername] [-e enablepassword]
[-s storagedevicename] [-c archive comments] [--overwrite|--no-overwrite] [--activate|--no-activate]
filename signalingpointname
```

**Command Description**

Uploads the specified GTT file to the specified ITP signaling point.

Use these keywords and arguments with this command. If you do not specify a required keyword or argument, the MWTM prompts you to specify it.

- **-l logfilename**—Writes detailed syntax and semantics checking results, as well as a detailed Telnet log, to the specified file.
- **-u username**—Log in username, if required by the ITP.

- **-p password**—Log in password, if required by the ITP.
- **-n enableusername**—Enable username, if required by the ITP.
- **-e enablepassword**—Enable password, if required by the ITP.
- **-s storagedevicename**—If the ITP has more than one storage device, uploads the file to the specified device, such as **disk1**, **flash**, or **slot2**.
- **-c archive comments**—Allows you to provide optional archive comments.
- **--overwrite**—If the specified file already exists on the specified ITP signaling point, overwrites the file.
- **--no-overwrite**—If the specified file already exists on the specified ITP signaling point, does not overwrite the file.
- **--activate**—Uploads the file and activates it (replaces the currently running file with the uploaded file).
- **--no-activate**—Uploads the file without activating it (does not replace the currently running file).

You must log in as the root user or superuser to use this command.

## mwtm pushmlr

### Server Only

#### Full Syntax

```
mwtm pushmlr [-l logfilename] [-u username] [-p password] [-n enableusername]
[-e enablepassword] [-s storagedevicename] [-c archive comments] [--overwrite|--no-overwrite]
[--activate|--no-activate] filename signalingpointname
```

#### Command Description

Uploads the specified address table file to the specified ITP signaling point.

Use these keywords and arguments with this command. If you do not specify a required keyword or argument, the MWTM prompts you to specify it.

- **-l logfilename**—Writes detailed syntax and semantics checking results, as well as a detailed Telnet log, to the specified file.
- **-u username**—Log in username, if the ITP requires.
- **-p password**—Log in password, if the ITP requires.
- **-n enableusername**—Enable username, if the ITP requires.
- **-e enablepassword**—Enable password, if the ITP requires.
- **-s storagedevicename**—If the ITP has more than one storage device, uploads the file to the specified device, such as **disk1**, **flash**, or **slot2**.
- **-c archive comments**—Allows you to provide optional archive comments.
- **--overwrite**—If the specified file already exists on the specified ITP signaling point, overwrites the file.
- **--no-overwrite**—If the specified file already exists on the specified ITP signaling point, does not overwrite the file.
- **--activate**—Uploads the file and activates it (replaces the currently running file with the uploaded file).

- **--no-activate**—Uploads the file without activating it (does not replace the currently running file).

You must log in as the root user or superuser to use this command.

## mwtm pushroute

### Server Only

#### Full Syntax

```
mwtm pushroute [-l logfile] [-u username] [-p password] [-n enableusername]
[-e enablepassword] [-s storagedevicename] [-c archive comments] [--overwrite|--no-overwrite]
[--activate|--no-activate] filename signalingpointname
```

#### Command Description

Uploads the specified route table file to the specified ITP signaling point.

Use these keywords and arguments with this command. If you do not specify a required keyword or argument, the MWTM prompts you to specify it.

- **-l logfile**—Writes detailed syntax and semantics checking results, as well as a detailed Telnet log, to the specified file.
- **-u username**—Log in username, if the ITP requires.
- **-p password**—Log in password, if the ITP requires.
- **-n enableusername**—Enable username, if the ITP requires.
- **-e enablepassword**—Enable password, if the ITP requires.
- **-s storagedevicename**—If the ITP has more than one storage device, uploads the file to the specified device, such as **disk1**, **flash**, or **slot2**.
- **-c archive comments**—Allows you to provide optional archive comments.
- **--overwrite**—If the specified file already exists on the specified ITP signaling point, overwrites the file.
- **--no-overwrite**—If the specified file already exists on the specified ITP signaling point, does not overwrite the file.
- **--activate**—Uploads the file and activates it (replaces the currently running file with the uploaded file).
- **--no-activate**—Uploads the file without activating it (does not replace the currently running file).

You must log in as the root user or superuser to use this command.

## mwtm q752stats

### Server Only

#### Full Syntax

```
mwtm q752stats [nodes] [linksets] [idtag] [quiet]
```

#### Command Description

Manually generates MWTM Q.752 statistics reports. To include:



- Or exclude specific objects in the reports, use the *nodes* argument. To include:
  - All nodes, specify **all**.
  - A single node or signaling point, specify a single node name, or node name and signaling point name, as the *nodes* argument. The node name must exactly match the node name that the MWTM discovered, including the domain name.

For example:

```
mwtm-75-59a.cisco.com
```

To specify a node name and signaling point:

```
mwtm-75-59a.cisco.com;net0
```

- Or exclude objects based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This is also the default setting for this command; you only need to specify **default** if you also want to specify an *idtag* or **quiet**.
- A group of nodes or signaling points other than the one specified in the *nodes.include* file, create a file that contains the list of nodes and signaling points to include and specify the full path and name of the file as the *nodes* argument.



**Note** For more details on including and excluding objects, see [Including or Excluding Specified Objects in ITP Reports, page 12-4](#).

If you specify *nodes*, you can also specify an *idtag* to identify the reports. The *idtag* can be any meaningful character string, but it cannot contain any spaces. The default value for *idtag* is the process ID of the **mwtm q752stats** command.

- Disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. The MWTM generates the report in export format, which you can view by using the MWTM web interface.

The first time you use the **mwtm q752stats** command to generate a report, you must enter the command at least twice. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful accounting statistics and, if the collected data appears valid, begins generating the report.

Thereafter, you only need to enter this command once to generate the report.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Customizing ITP Report Preferences, page 12-65](#)

## mwtm repcstage

### Server Only

#### Full Syntax

**mwtm repcstage** [*number-of-days*]

#### Command Description

Maximum number of days the MWTM should archive custom reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 10 days.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm repdir

### Server Only

#### Full Syntax

**mwtm repdir** [*directory*]

#### Command Description



#### Note

You must stop the MWTM server before performing this command. You are prompted whether to continue.

Sets the directory in which the MWTM stores report files. See [Chapter 12, “Managing Reports”](#) for information about MWTM reports.

The default directory for report files resides in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the default directory is */opt/CSCOs/gm/reports*.
- A different directory, then the default directory resides in that directory.

Use this command if you want to store report files in a different directory; for example, in a Network File System location on another server.

**Note**

This command copies all files in the current directory to the new directory. If you are not logged in as the superuser and you do not own the new directory, you might not be able to copy the files. In that case, you must specify a directory that you own or log in as the root user.

Do not set the new directory to any of these: */usr*, */var*, */opt*, or */tmp*.

Do not set the new directory to the same directory in which you are storing GTT files (**mwtm gttmdir**), message log files (**mwtm msglogdir**), route table files (**mwtm routedir**), or address table files (**mwtm atbldir**).

After you change the directory, the MWTM asks if you want to restart the MWTM server. The new directory takes effect when you restart the MWTM server.

You must log in as the root user or superuser to use this command.

## mwtm replog

### Server Only

### Full Syntax

**mwtm replog** [**clear** | **-r**]

### Command Description

Uses PAGER to display the contents of the system reports log. The reports log lists all messages that you use for the creation and maintenance of MWTM reports.

To clear the log and restart the server, enter **mwtm replog clear**.

To display the contents of the log in reverse order, with the most recent commands at the beginning of the log, enter **mwtm replog -r**.

The default path and filename for the system reports log file is */opt/CSCOs/gm/logs/sgmReportLog.txt*. If you installed the MWTM in a directory other than */opt*, then the system reports log file resides in that directory.

You must log in as the root user or superuser to use this command.

# mwtm routedir

## Server Only

### Full Syntax

**mwtm routedir** [*directory*]

### Command Description



#### Note

You must stop the MWTM server before performing this command. The system prompts you whether to continue.

Sets the DPC Route staging directory, the directory in which the MWTM stores ITP route table files, and enables Trivial File Transfer Protocol (TFTP) file transfer for the directory. See [Chapter 13, “Editing an ITP Route Table File”](#) for information about ITP route table files.

The default DPC Route staging directory resides in the MWTM installation directory. If you installed the MWTM in:

- The default directory, */opt*, then the directory is */opt/CSCOs/gm/routes*.
- A different directory, then the directory resides in that directory.

Use this command if you want to use a different DPC Route staging directory, such as */ftpboot* or a Network File System location on another server that is used as the Trivial File Transfer Protocol (TFTP) server for server configuration files for ITPs in the network.

This command copies all files in the current directory to the new directory. If you are not logged in as the superuser and do not own the new directory, the MWTM provides this prompt:

```
Can't create directory!! DPC Route Staging Directory not changed!!
```

```
Directory could be located on a remote NFS server.
Manually create directory and try again.
Set permissions using chmod 777.
```

You must specify a directory that you own, or you must log in as the root user. Do not set the new directory to any of these: */usr*, */var*, */opt*, or */tmp*.

Do not set the new directory to the same directory in which the GTT files (**mwtm gttmdir**), message log files (**mwtm msglogdir**), report files (**mwtm repdir**), or address table files (**mwtm atbldir**) reside.

When you enter this command, the MWTM also prompts you to enable TFTP file transfer for the DPC Route staging directory and for the TFTP path for the directory, **tftp://hostname/path**, where:

- *hostname* is the name or IP address of the host on which the DPC Route staging directory resides.  
If you enter a DNS name (such as **mwm-jumbo**) instead of an IP address (such as **172.18.12.10**), then the ITP must be able to resolve the DNS name; otherwise, when you try to deploy a file, the MWTM issues an appropriate error message and does not deploy the file.  
To enable the ITP to resolve DNS names, enter the **ip domain-lookup** command on the ITP. For more information about this command, see the *Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*, Release 12.3 or later.
- *path* is the path to the DPC Route staging directory.

After you change the directory or enable TFTP file transfer for the directory, the MWTM asks if you want to restart the MWTM server. The new directory and TFTP setting take effect when you restart the MWTM server.

You must log in as the root user or superuser to use this command.

**Note**

If you are setting up a new DPC Route staging directory on a Network File System location on another (remote) server, ensure that the server allows read-write access to the user account through which the MWTM runs and run this command as a superuser.

## mwtm routetabledefs

### Server Only

### Full Syntax

**mwtm routetabledefs** [**true** | **false**]

### Command Description

Specifies whether the MWTM should automatically populate the Route Table dialog box with default values:

- **true**—Automatically populate the Route Table dialog box with default values. This is the default setting.
- **false**—Do not automatically populate the Route Table dialog box with default values; that is, force the user to enter values in the dialog box.

When you enter this command, the new setting takes effect when you restart the MWTM server.

You must log in as the root user or superuser to use this command.

## mwtm start atblclient

### Server and all Clients

### Full Syntax

**mwtm start atblclient** [*hostname*]

### Command Description

Starts an MWTM Address Table Editor client on the specified host. If no hostname is specified, starts an MWTM Address Table Editor client on the default host, as specified during installation. See [Connecting to a New Server, page 5-43](#) for information about determining the default host.

If you access a remote workstation through Telnet, you must set the **DISPLAY** variable to your local display or you cannot use this command. If the **DISPLAY** variable is not set automatically, you must set it manually (see [Setting the DISPLAY Variable for Solaris or Linux Clients, page 4-3](#)).

This command has the same function as the **mwtm atblclient** command.

## mwtm start gttclient

### Server and all Clients

#### Full Syntax

**mwtm start gttclient** [*hostname*]

#### Command Description

Starts an MWTM GTT client on the specified host. If no hostname is specified, starts an MWTM GTT client on the default host, as specified during installation. See [Connecting to a New Server, page 5-43](#) for information about determining the default host.

If you access a remote workstation through Telnet, you must set the DISPLAY variable to your local display or you cannot use this command. If the DISPLAY variable is not set automatically, you must set it manually (see [Setting the DISPLAY Variable for Solaris or Linux Clients, page 4-3](#)).

This command has the same function as the **mwtm gttclient** command.

## mwtm statreps acct

### Server Only

### Full Syntax

**mwtm statreps** [**acct** | **noacct**]

### Command Description

Specifies whether the MWTM should generate MTP3 and XUA accounting reports. MTP3 accounting describes MTP3 layer traffic in support of linksets; XUA accounting describes MTP3 layer traffic in support of application servers.

- **acct**—Generate MTP3 and XUA accounting reports. You must enable MTP3 accounting on the links for the MWTM to generate MTP3 accounting reports.
- **noacct**—Do not generate MTP3 or XUA accounting reports. This is the default setting.



### Note

This command does not trigger the immediate collection of statistics. By default, MWTM collects MTP3 and XUA accounting statistics nightly. It might take up to 2 days before the first reports are generated.

See [MTP3 Accounting Reports, page 12-42](#) for more information on MTP3 accounting reports. See [AS/ASP Accounting Reports, page 12-44](#), for more information on XUA accounting reports.

You must log in as the root user or superuser to use this command.

## mwtm statreps clean

### Server Only

### Command Description

Removes all data from MWTM network statistics reports, restoring the reports to an unchanged state.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps cleancustom

### Server Only

### Full Syntax

**mwtm statreps cleancustom** [*tag*]

### Command Description

Removes all data from one or more MWTM custom statistics reports, restoring the reports to an unchanged state. To clean:

- All custom reports, enter **mwtm statreps cleancustom**.
- A single custom report, enter **mwtm statreps cleancustom** *tag*, where *tag* is the ID tag of the custom report that you want to clean.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps custage

### Server Only

### Full Syntax

**mwtm statreps custage** [*number-of-days*]

### Command Description

Maximum number of days the MWTM should archive custom reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 10 days.

This command has the same function as the **mwtm repcustage** command.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)



## mwtm statreps dailyage

### Server Only

### Full Syntax

**mwtm statreps dailyage** [*number-of-days*]

### Command Description

Maximum number of days the MWTM should archive daily network statistics reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 90 days.

This command has the same function as the **mwtm repdailyage** command.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps diskcheck

### Server Only

### Full Syntax

**mwtm statreps** [**diskcheck** | **nodiskcheck**]

### Command Description

Specifies whether the MWTM should verify that a disk has at least 10 MB of space remaining before generating network statistics reports:

- **diskcheck**—Verify the disk space. This is the default setting.
- **nodiskcheck**—Do not verify the disk space.

If your system does not return the necessary amount of free space, in a correct format that the MWTM can parse, use this command to disable checking to allow reporting to continue.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps enable

### Server Only

#### Full Syntax

**mwtm statreps** [**disable** | **enable**]

#### Command Description

Use to generate network statistics and accounting reports:

- **enable**—Generate network statistics and accounting reports. This is the default setting.
- **disable**—Do not generate network statistics and accounting reports.

You must enter this command to generate network statistics and accounting reports before entering the **mwtm accstats**, **mwtm gttstats**, **mwtm linkstats**, **mwtm mlrstats**, and **mwtm xuastats** commands.

See [Chapter 12, “Managing Reports”](#) for more information on network statistics and accounting reports.

You must log in as the root user or superuser to use this command.

## mwtm statreps export

### Server Only

#### Full Syntax

**mwtm statreps** [**export** | **noexport**]

#### Command Description

Specifies whether the MWTM should generate network statistics and accounting reports in export format:

- **export**—Generate network statistics reports in export format. This is the default setting.
- **noexport**—Do not generate network statistics reports in export format.

Network statistics reports in export format are *.zip* files that contain comma-separated value (CSV) text files that you can download and unzip.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Generating Reports, page 12-1](#)

## mwtm statreps gtt

### Server Only

### Full Syntax

**mwtm statreps** [**gtt** | **nogtt**]

### Command Description

Specifies whether the MWTM should generate GTT accounting statistics reports:

- **gtt**—Generate GTT accounting statistics reports. You must enable GTT accounting for the MWTM to generate GTT accounting statistics.
- **nogtt**—Do not generate GTT accounting statistics reports. This is the default setting.



### Note

This command does not trigger immediate collection of statistics. By default, MWTM collects GTT accounting statistics nightly. It might take up to 2 days before the first reports are generated.

See [GTT Accounting Reports, page 12-41](#) for more information on GTT accounting statistics reports.

You must log in as the root user or superuser to use this command.

## mwtm statreps hourlyage

### Server Only

### Full Syntax

**mwtm statreps hourlyage** [*number-of-days*]

### Command Description

Maximum number of days the MWTM should archive hourly network statistics reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 31 days.

This command has the same function as the **mwtm rephourlyage** command.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps iplinks

### Server Only

### Full Syntax

**mwtm statreps** [**iplinks** | **noiplinks**]

### Command Description

Specifies whether the MWTM should include links that use the Stream Control Transmission Protocol (SCTP) IP transport protocol in network statistics reports:

- **iplinks**—Include SCTPIP links. This is the default setting.
- **noiplinks**—Do not include SCTPIP links.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps link

### Server Only

### Full Syntax

**mwtm statreps** [**link** | **nolink**]

### Command Description

Specifies whether the MWTM should generate link and linkset statistics summary reports:

- **link**—Generate link and linkset statistics summary reports.
- **nolink**—Do not generate link and linkset statistics summary reports. This is the default setting.



### Note

This command does not trigger immediate collection of statistics. By default, MWTM collects link and linkset statistics hourly. It might take up to 2 hours before the first reports are generated. See [Link Reports, page 12-17](#) and [Linkset Reports, page 12-23](#) for more information on link and linkset statistics summary reports.

You must log in as the root user or superuser to use this command.

## mwtm statreps maxcsvrows

### Server Only

#### Full Syntax

**mwtm statreps maxcsvrows** [rows]

#### Command Description

Specifies the maximum number of rows that the MWTM includes in export CSV files:

- **rows**—Maximum number of rows to include.



**Note** If you want to limit export CSV files to a size that Microsoft Excel can handle, set the value to 65535.

This command only applies to these files:

- *MWTMLinksetStats.RollingSevenDayAllHours.csv.zip*
- *MWTMLinkStats.RollingSevenDayAllHours.csv.zip*
- *MWTMAccStats.DailyDetail.<yyyy-mm-dd>.csv.zip*

See [Rolling Archived Reports, page 12-49](#) and [Daily MTP3/AS Accounting Statistics Archived Reports, page 12-44](#) for more information on affected CSV files.

You must log in as the root user or superuser to use this command.

## mwtm statreps mlr

### Server Only

#### Full Syntax

**mwtm statreps** [mlr | nomlr]

#### Command Description

Specifies whether the MWTM should generate MLR accounting reports:

- **mlr**—Generate MLR reports. You must also enable MLR reporting for the MWTM to generate MLR reports.
- **nomlr**—Do not generate MLR reports. This is the default setting.



**Note** This command does not trigger immediate collection of statistics. By default, MWTM collects MLR accounting statistics nightly. It might take up to 2 days before the first reports are generated.

See [MLR Reports, page 12-27](#) for more information on MLR reports.

You must log in as the root user or superuser to use this command.

## mwtm statreps msu

### Server Only

### Full Syntax

**mwtm statreps** [**msu** | **nomsu**]

### Command Description

Specifies whether the MWTM should generate MSU rates reports:

- **msu**—Generate MSU rates reports. You must also enable reporting for the MWTM to generate MSU rates reports.
- **nomsu**—Do not generate MSU rates reports. This is the default setting.

See [MSU Rates Reports, page 12-32](#) for more information on MSU rates reports.

You must log in as the root user or superuser to use this command.

## mwtm statreps nullcaps

### Server Only

### Full Syntax

**mwtm statreps** [**nullcaps** | **nonnullcaps**]

### Command Description

Specifies whether the MWTM should include SCTP links that do not have planned send and receive capacities in network statistics reports:

- **nullcaps**—Include SCTP links that do not have planned send and receive capacities. This is the default setting.
- **nonnullcaps**—Do not include SCTP links that do not have planned send and receive capacities.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps q752

### Server Only

### Full Syntax

**mwtm statreps** [**q752** | **noq752**]

### Command Description

Specifies whether the MWTM should generate Q.752 daily statistics reports:

- **q752**—Generate Q.752 statistics reports.
- **noq752**—Do not generate Q.752 statistics reports. This is the default setting.



### Note

This command does not trigger immediate collection of statistics. By default, MWTM collects Q.752 statistics nightly. It might take up to 2 days before the first reports are generated.

You must log in as the root user or superuser to use this command.

## mwtm statreps servratio

### Server Only

### Full Syntax

**mwtm statreps servratio** [*factor*]

### Command Description

Displays a red ball in the In-Service cell in a network statistics report, if this condition is met:

$$\text{Current In-Service} < \text{factor} * \text{Long-Term In-Service}$$

The default value for *factor* is **0.95**. Therefore, when the percentage of time that a link is in service (for an hour) falls below 95% of the long-term in-service percentage for that link, a red ball appears in the In-Service cell.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps status

### Server Only

### Command Description

Displays the current status of all MWTM network statistics report parameters. You use the other **mwtm statreps** commands, such as **mwtm statreps [disable | enable]** and **mwtm statreps [diskcheck | nodiskcheck]** to set these parameters.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)



## mwtm statreps timemode

### Server Only

### Full Syntax

**mwtm statreps timemode** [12 | 24]

### Command Description

Sets the time mode for dates in network statistics reports:

- **12**—Use 12-hour clock, with AM and PM. 1:00 in the afternoon is 1:00 PM.
- **24**—Use 24-hour clock, also called military time. 1:00 in the afternoon is 13:00. This is the default setting.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps timer

### Server Only

### Command Description

Displays the timer file for MWTM network statistics reports. The timer file is useful for identifying how much time the MWTM spends gathering report data and generating reports.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps utilratio

### Server Only

#### Full Syntax

**mwtm statreps utilratio** [*factor*]

#### Command Description

Displays a red ball in the Send Utilization or Receive Utilization cell in a network statistics report, if this condition is met:

**Current Utilization** > *factor* \* **Long-Term Utilization**

The default value for *factor* is **1.50**. Therefore, if the link utilization for a particular hour is more than 150% of the long-term average for that link, the red ball appears in the Send Utilization or Receive Utilization cell.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps xua

### Server Only

#### Full Syntax

**mwtm statreps** [*xua* | *noxua*]

#### Command Description

Specifies whether the MWTM should generate statistics reports for application servers and application server processes:

- **xua**—Generate statistics reports for application servers and application server processes.
- **noxua**—Do not generate statistics reports for application servers and application server processes. This is the default setting.



#### Note

This command does not trigger immediate collection of statistics. By default, MWTM collects xUA statistics hourly. It might take up to 2 hours before the first reports are generated.

See [Application Server Reports, page 12-9](#) and [Application Server Process Reports, page 12-12](#) for more information on statistics reports for application servers and application server processes.

You must log in as the root user or superuser to use this command.

## mwtm xuastats

### Server Only

### Full Syntax

**mwtm xuastats** [*nodes* [*idtag*]] [*sortopts*] [**quiet**]

### Command Description

Generates MWTM accounting statistics reports for application servers and application server processes. To:

- Include or exclude specific objects in the reports, use the *nodes* argument. To include:
  - All nodes, specify **all**.
  - A single node or signaling point, specify a single node name, or node name and signaling-point name, as the *nodes* argument. The node name must exactly match the node name that the MWTM discovered, including the domain name, and each line must end with a colon (:).

For example:

```
mwtm-75-59a.cisco.com:
```

To specify a node name and signaling point:

```
mwtm-75-59a.cisco.com;net0:
```

- Or exclude objects based on the contents of the user-defined *nodes.include*, *linksets.include*, *nodes.exclude*, and *linksets.exclude* files, create the files, then specify **default**. This is also the default setting for this command; you only need to specify **default** if you also want to specify an *idtag*, *sortopts*, or **quiet**.
- A group of nodes or signaling points other than the one specified in the *nodes.include* file, create a file that contains the list of nodes and signaling points to include and specify the full path and name of the file as the *nodes* argument.



#### Note

For more details on including and excluding objects, see [Including or Excluding Specified Objects in ITP Reports, page 12-4](#).

If you specify *nodes*, you can also specify an *idtag* to identify the reports. The *idtag* can be any meaningful character string, but it cannot contain any spaces. The default value for *idtag* is the process ID of the **mwtm xuastats** command.

- Specify the sort order for an application server report, specify one of these keywords for the *sortopts* argument:
  - **-sfm**—Sort based on the Packets From MTP3 column, in descending order. This is the default setting.
  - **-sta**—Sort based on the Packets To ASPs column, in descending order.
- Specify the sort order for an application server process report, specify one of these keywords for the *sortopts* argument:
  - **-sfa**—Sort based on the Packets From ASPs column, in descending order. This is the default setting.
  - **-sfm**—Sort based on the Packets From MTP3 column, in descending order.

- **-sre**—Sort based on the Receive Errors column, in descending order.
- **-sse**—Sort based on the Send Errors column, in descending order.
- **-sta**—Sort based on the Packets To ASPs column, in descending order.
- **-stm**—Sort based on the Packets To MTP3 column, in descending order.
- Disable automatic output to the terminal when running this command in a script, specify the **quiet** keyword. The MWTM generates the report in export format, which you can view by using the MWTM web interface.

Before entering this command, you must enable the MWTM to generate accounting statistics reports for application servers and application server processes. See the description of the **mwtm statreps** [**xua** | **noxua**] command for more information.

The first time you use the **mwtm xuastats** command to generate a report, you must enter the command at least twice. The:

- First entry gets the first set of raw data.
- Second entry begins calculating useful accounting statistics and, if the collected data appears valid, begins generating the report.

Thereafter, you need only enter this command once to generate the report.

You must log in as the root user or superuser to use this command.

#### Related Topic

[Application Server Reports, page 12-9](#)

## RAN-O-Only Commands

RAN-O-only commands include:

- [mwtm rep15minage, page B-130](#)
- [mwtm repmonthlyage, page B-131](#)
- [mwtm statreps 15minage, page B-131](#)
- [mwtm statreps monthlyage, page B-132](#)

### mwtm rep15minage

#### Server Only

#### Full Syntax

**mwtm rep15minage** [*number-of-days*]

#### Command Description

Maximum number of days the MWTM should archive 15-minute reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 31 days.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Locating Stored ITP Reports, page 12-63](#)

## mwtm repmonthlyage

**Server Only****Full Syntax**

**mwtm repmonthlyage** [*number-of-days*]

**Command Description**

Maximum number of days the MWTM should archive monthly reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 3650 days.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps 15minage

**Server Only****Full Syntax**

**mwtm statreps 15minage** [*number-of-days*]

**Command Description**

Maximum number of days the MWTM should archive 15-minute network statistics reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 31 days.

This command has the same function as the **mwtm rep15minage** command.

You must log in as the root user or superuser to use this command.

**Related Topic**

[Locating Stored ITP Reports, page 12-63](#)

## mwtm statreps monthlyage

### Server Only

### Full Syntax

**mwtm statreps monthlyage** [*number-of-days*]

### Command Description

Maximum number of days the MWTM should archive monthly network statistics reports.

If you enter this command without the *number-of-days* argument, the MWTM displays the current maximum number of days. You can then change that value or leave it. The valid range is 1 day to an unlimited number of days. The default value is 3650 days.

This command has the same function as the **mwtm repmonthlyage** command.

You must log in as the root user or superuser to use this command.

### Related Topic

[Locating Stored ITP Reports, page 12-63](#)



# APPENDIX C

## FAQs

---

This appendix contains:

- [General FAQs, page C-1](#)
- [ITP Specific FAQs, page C-13](#)
- [RAN-O Specific FAQs, page C-17](#)

## General FAQs

These categories of frequently asked questions are general questions about the Cisco Mobile Wireless Transport Manager (MWTM):

- [Installation Questions, page C-1](#)
- [Server Questions, page C-2](#)
- [GUI Questions, page C-5](#)
- [Browser Questions, page C-6](#)
- [Topology Questions, page C-6](#)
- [Events and Alarms Questions, page C-7](#)
- [Polling Questions, page C-8](#)
- [MIB Questions, page C-9](#)
- [Miscellaneous Questions, page C-9](#)

## Installation Questions

This section addresses the following installation questions:

- [How do I install the MWTM client?, page C-2](#)
- [After a failed uninstall of the Windows client, I am prompted to uninstall again, but the procedure does not work. Why?, page C-2](#)
- [Why do I see strange character strings when I install the MWTM?, page C-2](#)

**How do I install the MWTM client?**

You can install the MWTM client either from the DVD distributed with the MWTM, or by using a web browser to download the MWTM client from an MWTM server. See the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1* for full details.

**After a failed uninstall of the Windows client, I am prompted to uninstall again, but the procedure does not work. Why?**

If for some reason the Windows MWTM client uninstall procedure fails before the client is completely uninstalled, the MWTM prompts you to uninstall the client again. However, this might not be possible using the standard **Add/Remove Programs** icon in the Windows Control Panel, or from the Windows Start menu.

If you cannot uninstall the MWTM client using the standard procedure, use this procedure:

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Delete the MWTM client installation directory and its contents. If you installed the MWTM client in the default directory, <i>C:\Program Files</i> , then the installation directory is <i>C:\Program Files\Cisco Systems\MWTM Client</i> . If you installed the MWTM client in a different directory, then the installation directory resides in that directory. |
| <b>Step 2</b> | Delete the MWTM Client entries from the Windows Start menu and desktop.                                                                                                                                                                                                                                                                                           |
- 

**Why do I see strange character strings when I install the MWTM?**

Some UNIX systems use the LANG variable to indicate the locale. The setting of the LANG environment variable can cause syntax errors in the MWTM setup scripts, which can result in messages that contain strange character strings such as `?y?d@O`. To correct this problem, unset the LANG environment variable in the workstation from which you are installing the MWTM, using one of these commands:

- If you are running sh, enter the **unset LANG** command.
- If you are running csh, enter the **unsetenv LANG** command.

Then install the MWTM again.

## Server Questions

This section addresses the following server questions:

- [What workstation and network devices do I need to run the MWTM?, page C-3](#)
- [Why can't my remote workstation access the MWTM on my local workstation?, page C-3](#)
- [I moved the server on which I had installed the MWTM and now I can't start the MWTM client or server. Why?, page C-3](#)
- [Why did I receive a "cannot connect to server" message?, page C-4](#)
- [Will the MWTM server processes restart automatically after a system reboot?, page C-5](#)
- [Why doesn't my MWTM server start after installing SSL?, page C-5](#)



**What workstation and network devices do I need to run the MWTM?**

The MWTM comprises two distinct pieces of functionality.

- The MWTM server application runs on Solaris/Linux only.
- The MWTM client application, including the user interface, runs on Solaris/Linux and Windows XP Professional. For Solaris/Linux, the MWTM client can run on the same system as the MWTM server, or on a different system.

**Note**

The Linux client is unsupported.

For further hardware and software requirements, see the “Preparing to Install the MWTM” chapter of the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.

**Why can't my remote workstation access the MWTM on my local workstation?**

Keep in mind that performance is always better if you access the MWTM by installing the MWTM client on the remote workstation.

However, if you want to enable a remote Solaris/Linux workstation to access the MWTM on a local workstation, enter the **xhost + remote\_workstation** UNIX command on your local workstation, where *remote\_workstation* is the remote device you are enabling to access your local workstation.

To enable a remote Windows workstation to access the MWTM on a local workstation, you can use an X-Window system emulator such as eXceed or Reflection X, but be aware that there might be display problems. For example, the window borders might disappear, or the keyboard focus might be missing.

The **X Performance Enhancer (AntiAliasing Off)** check box in the Preferences window specifies whether antialiasing is turned on in the topology map. Antialiasing, which is turned on by default, improves the appearance of the icons and connections in the map.

You can improve the performance of the MWTM client on a remote workstation by turning off antialiasing in the topology map. For more information, see [Turning Off Antialiasing, page 10-25](#).

**I moved the server on which I had installed the MWTM and now I can't start the MWTM client or server. Why?**

If you change the IP address of the server on which you installed the MWTM, or if you move the server to a new network, you must reboot the server to prevent MWTM connection problems.

To reboot the server, use this procedure:

**Step 1** Log in as the root user, as described in [Becoming the Root User \(Server Only\), page 4-2](#).

**Step 2** Enter:

```
cd /opt/CSCOsgm/bin
./mwtm reboot
```

If you change the server's Solaris/Linux hostname, you must reset the default hostname on the MWTM server and client, using this procedure:

**Step 3** Log in as the root user, as described in [Becoming the Root User \(Server Only\), page 4-2](#).

**Step 4** Enter:

```
cd /opt/CSCOsgm/bin
./mwtm evilstop
```

The MWTM stops all MWTM servers on the local host.

**Step 5** Enter:

```
./mwtm servername hostname
```

where *hostname* is the new default hostname. Ensure that the new name is valid and is defined in your */etc/hosts* file.

The MWTM resets the default hostname for the MWTM server and client and automatically restarts the MWTM server.

**Step 6** Any remote clients connecting to this new host should also change their default server name. From Windows, choose **Start > Programs > Cisco MWTM Client > Modify Default MWTM Server Name**.**Why did I receive a “cannot connect to server” message?**

When you launch the MWTM client, the GTT Editor, Address Table Editor, or the Event Editor, or when you connect to a new server (whether manually or automatically as the result of a server failure), you might receive this message:

This client is not allowed to connect to the server or the server is listening on a port the client does not know about or cannot reach. Click the help button for a more detailed explanation.

If you receive this message, one of these situations has occurred:

- An MWTM administrator has prevented your MWTM client from connecting to the MWTM server, using the **mwtm ipaccess** command.

To resolve this problem, contact the MWTM administrator and ask to have your client's IP address added to the *ipaccess.conf* file (see [Limiting MWTM Client Access to the MWTM Server \(Server Only\)](#), page 2-31).

- The MWTM server has more than one IP address, but the MWTM server's default hostname is set to an IP address that your MWTM client cannot access.

To resolve this problem in Solaris/Linux, use the **mwtm servername** command to reset the MWTM server's default hostname to an IP address that your client can access and restart the server (see [mwtm servername](#), page B-57).

To resolve this problem in Windows, choose **Start > Programs > Cisco MWTM Client > Modify Default MWTM Server Name**, then you can enter the **mwtm servername** command.



**Note** Using the **mwtm servername** command to reset the MWTM server's default hostname does not affect communication between the MWTM server and the nodes.

- A firewall is installed between the MWTM server and your MWTM client that only allows traffic to pass through to the MWTM server's port numbers 1774 (the MWTM web server port) and 44742 (the MWTM Naming server port), but communication between the MWTM servers and clients requires additional ports.

To resolve this problem, set up the firewall correctly (see [Firewall Communication](#), page H-6).

**Will the MWTM server processes restart automatically after a system reboot?**

Yes. When you install the MWTM server, the MWTM modifies your system startup scripts to ensure that the MWTM server processes start up again after a system reboot. To accomplish this, the MWTM adds these lines to your system startup scripts:

```
/etc/init.d/sgm
/etc/rc0.d/K99sgm
/etc/rc1.d/K99sgm
/etc/rc2.d/K99sgm
/etc/rc3.d/K99sgm
/etc/rc3.d/S99sgm
```

These lines ensure that the MWTM shutdown and startup scripts run in the correct order for each system initiation state.

Note that for Linux only, these lines are modified as well:

```
/etc/rc5.d/S99sgm
/etc/rc6.d/K99sgm
```

**Why doesn't my MWTM server start after installing SSL?**

If you have not installed the SSL key and certificate, the MWTM server will not start. For exact details on this process, see [Enabling SSL Support on the MWTM Server, page 2-22](#).

## GUI Questions

This section addresses the following GUI questions:

- [Some of my MWTM windows are showing up with small, unusable text entry fields. How can I correct this?, page C-5](#)
- [Sometimes my MWTM display seems to lock up. Why?, page C-5](#)

**Some of my MWTM windows are showing up with small, unusable text entry fields. How can I correct this?**

Depending on your system, as well as other factors, the MWTM windows can sometimes display so small that text is illegible, and columns and text entry fields are very narrow and unusable. If this happens, resize the window and widen the individual columns until the information is again legible and the columns and text entry fields are usable.

To make a column wider or narrower, click the column divider in the heading and move the divider to the right or left while holding down the right mouse button.

**Sometimes my MWTM display seems to lock up. Why?**

In the MWTM, events might cause message popups to remain in the background of your display, preventing you from interacting with other windows. If you suspect that your display has locked up, perform these tasks:

- Ensure that you are running the MWTM on a supported operating system. For more information about supported operating systems, see “Preparing to Install the MWTM” in the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.
- Minimize windows and look for an MWTM message popup in the background.

## Browser Questions

This section addresses the following browser questions:

- [Sometimes when browsing the MWTM web interface, a popup appears with this message: Unresponsive Script. Why does this happen and how can I prevent it from reoccurring?, page C-6](#)
- [The MWTM web pages appear empty \(without content\). Why does this happen and how can I prevent it from reoccurring?, page C-6](#)

**Sometimes when browsing the MWTM web interface, a popup appears with this message: Unresponsive Script. Why does this happen and how can I prevent it from reoccurring?**

This problem occurs when using the Firefox browser version 1.5. It is not an MWTM bug. You can prevent the popup from occurring with this workaround:

- 
- Step 1** In the address bar of a Firefox browser window, enter **about:config**
- Step 2** In the filter bar, enter **dom.max\_script\_run\_time**.
- Step 3** You should now see a setting appear in the window below the filter bar. The setting's name should match what you entered previously (dom.max\_script\_run\_time) and most likely shows a default value of 5.
- Step 4** Double-click this setting. Firefox will prompt you for a new value. Enter **10**.
- If changing this setting still causes the Unresponsive Script popup to appear, repeat these steps but increase the number that you enter in this step.
- 

**The MWTM web pages appear empty (without content). Why does this happen and how can I prevent it from reoccurring?**

Your Internet Explorer browser settings in the MWTM client are disabling active scripting. To modify this, in Internet Explorer, change the browser settings as follows:

- 
- Step 1** Choose **Tools > Internet Options**.
- Step 2** Select the Security tab.
- Step 3** Click the **Custom Level** button.
- Step 4** Search for Active Scripting in the Scripting section.
- Step 5** Click the **Enable** radio button to enable Active Scripting.
- Step 6** Search for Logon in the User Authentication section.
- Step 7** Click the **Automatic Logon with current username and password** radio button.
- 

## Topology Questions

This section addresses the following topology questions:

- [How does “zoom in on an area” work in a topology map?, page C-7](#)
- [Can I add my own icons to the topology map?, page C-7](#)

**How does “zoom in on an area” work in a topology map?**

With this feature, you can zoom in on a chosen area of the topology map in the topology window. To do so, click the **Zoom in on an area** button, or choose **Topology Tools > Zoom > Area** from the MWTM main menu, then click in the topology map and drag a rectangle around the area you want to zoom in on. The MWTM expands the chosen area to fill the topology map.

**Can I add my own icons to the topology map?**

No. To ensure that icons on the topology map can be resized cleanly, they are drawn as special vector-based images. Raster images, such as GIF files, do not resize cleanly.

## Events and Alarms Questions

This section addresses the following events and alarms questions:

- [If I select the Clear Event Icon menu option, does that delete the event from the MWTM database?, page C-7](#)
- [Can I add my own sounds to the Event Sound Filter?, page C-7](#)
- [Why are the age of my alarms always 0 minutes?, page C-8](#)
- [Why are objects in the Physical folder ignored?, page C-8](#)

**If I select the Clear Event Icon menu option, does that delete the event from the MWTM database?**

No. When you select the **Clear Event Icon** menu option for an object, the MWTM does not delete the actual event from its database. The MWTM only deletes the event icon (an orange triangle) from its displays for the object, and only for the MWTM client on which you are currently working.

**Can I add my own sounds to the Event Sound Filter?**

Yes. You can add sound files to an MWTM client. The MWTM clients can play these sound file formats: AIFC, AIFF, AU, SND, and WAV.

**Note**


---

WAV files encoded using MPEG Layer-3 are not supported.

---

The MWTM client sound files are stored in the MWTM client's *sounds* directory:

- If you installed the MWTM client for Solaris/Linux in the default directory, */opt*, then the sound file directory is */opt/CSCOsgmClient/sounds*.
- If you installed the MWTM client for Windows in the default directory, */Program Files*, then the sound file directory is *C:\Program Files\Cisco Systems\MWTM Client\sounds*.
- If you installed the MWTM in a different directory, then the sound file directory resides in that directory.

If for some reason the MWTM cannot play a specified sound file, the MWTM plays a default beep. For example, the MWTM cannot play a sound file if one of these conditions exists:

- The file has been moved or deleted from the *sounds* directory.
- The *sounds* directory has been deleted or cannot be found.
- Some other application is using all of the sound resources.
- No sound card is present.

**Why are the age of my alarms always 0 minutes?**

If the server clock is ahead of the client clock, the value will be 0 until the client clock catches up to the server clock. To get accurate values, use a time service such as Network Time Protocol (NTP) or similar, which keeps server and client clocks in sync.

**Why are objects in the Physical folder ignored?**

Interfaces that are not configured for ITP, IPRAN, mSEF, or management connections could be set as administratively up on the node; however, since these interfaces are not connected and/or not configured, they appear to be operationally down, even though this status does not affect the behavior of the network (for example, unconnected E1 ports on cards in an ONS chassis). To make sure that these interfaces do not contribute to the overall status of the parent node, the Physical folder status is ignored.

Objects that appear in the Physical folder but also outside of the Physical folder are *not* ignored, and their status does contribute to the status of the parent node.

If you want to monitor the status of objects that are ignored in the Physical folder:

- 
- Step 1** In the MWTM client navigation tree, expand the node that contains the Physical folder you want to unignore. Right-click and choose **Physical > Unignore**.
- Step 2** In the Status Contributors tab for the Physical folder, in the Ignored column, check the boxes for the objects you want to keep ignoring. Only the objects with unchecked boxes will be unignored.
- 

## Polling Questions

This section addresses the following polling questions:

- [How often does the MWTM poll nodes?, page C-8](#)
- [How do I change the default status polling interval?, page C-8](#)

**How often does the MWTM poll nodes?**

By default, the MWTM polls the nodes in the network every 15 minutes. However, you can initiate a poll for one or more nodes at any time by selecting the nodes in the Discovery tab in the Discovery dialog box and pressing **Poll**.

You can also change the default poll interval for one or more nodes in the SNMP Configuration dialog box. You must be logged in as the root user or as a superuser to access this dialog box.

Finally, the Node Details window polls the visible node and its adjacent node every 15 seconds, but you can change that poll interval, too.

**How do I change the default status polling interval?**

The MWTM polls the MWR node for status information (for example, interface up or down) every 15 minutes. The size of this poll depends on the number and type of interfaces that are enabled on the MWR.

To change the default polling interval of 15 minutes, open the SNMP Configuration dialog box by selecting **Network > SNMP Configuration** from the MWTM main window. You can use this dialog box to change the default polling interval to any number of minutes from 5 to 1440.

**Note**

The status information in the GUI is only as good as the most recent poll.

## MIB Questions

### What are the names of the MIBs used by the MWTM?

You can find the complete list of MIBs that the MWTM configures and queries in [Appendix F, “MIB Reference.”](#)

You can obtain the latest versions of these MIBs from one of these locations:

- The Zip file *mibs.zip*, located at the top of the MWTM DVD Image, contains these MIBs.
- You can download these MIBs from the Cisco website:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

## Miscellaneous Questions

This section addresses the following miscellaneous questions:

- [Does the MWTM require any other NMS applications?, page C-9](#)
- [Can I run the MWTM on my Windows PC?, page C-9](#)
- [What is a superuser?, page C-10](#)
- [Does the MWTM Java RMI use TCP or UDP?, page C-10](#)
- [What does this message mean: MessageLoggerProxy:setMessageLogger\(\): Could not resolve., page C-10](#)
- [What does a status of Deleted, Uninhibited, or NoShutdown mean?, page C-10](#)
- [Why don't the contents of the syslog tab match the log files of my syslog server?, page C-10](#)
- [When I start my MWTM client, I get a login window. However, I did not specify a user password during installation. How do I fix this?, page C-10](#)
- [I'm field testing MWTM in my lab and I see confusing results when discovering new network configurations. What's going on?, page C-12](#)

### Does the MWTM require any other NMS applications?

The MWTM is functionally a standalone product and does not require any other products. However, you can integrate the MWTM with other products to provide added value.

For example, you can integrate the MWTM with CiscoWorks, which provides access to the full suite of CiscoWorks products, including the Device Center, the CiscoView Element Manager, Resource Manager Essentials (RME), the Internetwork Performance Monitor (IPM), the Access Control List Manager, the Content Services Gateway (CSG) Service Manager, and the GPRS Gateway Support Node (GGSN) Service Manager. See [Integrating the MWTM with CiscoWorks, page 5-39](#) for more information.

You can also forward the MWTM events to other hosts, in the form of SNMP traps. This enables the MWTM to integrate with high-level event- and alarm-monitoring systems such as the Cisco Info Center (CIC) and Micromuse's Netcool suite of products. These systems can provide a single high-level view of all alarm monitoring in your network, making it easier to detect and resolve problems (see [Forwarding Events as Traps to Other Hosts, page 9-48](#)).

### Can I run the MWTM on my Windows PC?

You can run the MWTM client on Windows XP Professional on your PC. However, the MWTM server must run on a Solaris/Linux system.

**What is a superuser?**

A superuser is an MWTM user who has been enabled to perform most of the MWTM functions that otherwise require the user to be logged in as the root user.

For a complete description of the functions that a superuser can and cannot perform, as well as instructions for enabling a superuser, see [Specifying a Super User \(Server Only\)](#), page 2-20.

**Does the MWTM Java RMI use TCP or UDP?**

The two-way RMI communication in the MWTM that occurs between Java-based GUI clients and Java-based server processes uses TCP sockets.

**What does this message mean: `MessageLoggerProxy:setMessageLogger(): Could not resolve`.**

One of these conditions has occurred:

- The host or port number of the Message Log server is configured incorrectly. Verify that the host or port number is valid.
- The MWTM cannot reach the Message Log server, probably because it is restarting. The MWTM recovers the connection when the Message Log server restarts.

**What does a status of Deleted, Uninhibited, or NoShutdown mean?**

A status of Deleted, Uninhibited, or NoShutdown indicates a possible problem with the MWTM. If you see one of these status settings, contact Cisco TAC or your Cisco Account Team.

**Why don't the contents of the syslog tab match the log files of my syslog server?**

The MWTM client shows current syslog information available from a node, which reflects what content the node has stored in its internal memory. It is possible to configure your node to send its syslog messages to a host that stores these messages in files (usually under `/var/adm`). The MWTM does not access these persisted log messages, even if the host on which your MWTM server is running is logging syslog messages from your node. To access these persisted log messages, use CiscoWorks, or other software with syslog viewing capabilities.

**When I start my MWTM client, I get a login window. However, I did not specify a user password during installation. How do I fix this?**

When you install the MWTM and if you select all the default settings, user security is enabled (default option) which causes the MWTM login window to appear when you start the MWTM client. However, if you did not provide a user password during the installation, you must disable user security before you can log into the MWTM client or add user passwords to the MWTM.



To *disable* user security:

---

**Step 1** Log in as the root user on the MWTM server.

**Step 2** Run the following command:

```
/opt/CSCOsgrm/bin/mwtm useraccess disable
```

Output similar to the following appears:

```
[root@mwtm-server bin]# /opt/CSCOsgrm/bin/mwtm useraccess disable
```

```
User Based Access Protection is Disabled.
MWTM server must be restarted for changes to take effect.
Use the following command to restart the server:
```

```
mwtm restart
```

```
Clear browser cache and restart browser after changing MWTM Security!!
[root@mwtm-server bin]#
```

**Step 3** Make sure you restart the MWTM server (using the **mwtm restart** command) to activate the new security settings.

---

To *enable* user security:

---

**Step 1** Log in as the root user on the MWTM server.

**Step 2** Run the following command:

```
/opt/CSCOsgrm/bin/mwtm useraccess enable
```

**Step 3** Run the following command:

```
/opt/CSCOsgrm/bin/mwtm adduser <username>
```

Output similar to the following appears:

```
[root@mwtm-server bin]# /opt/CSCOsgrm/bin/mwtm useraccess enable
```

```
User Based Access Protection is Enabled.
Use the "mwtm adduser" command to add users.
Log in with usernames and passwords for access to MWTM Features.
MWTM server must be restarted for changes to take effect.
Use the following command to restart the server:
```

```
mwtm restart
```

```
Clear browser cache and restart browser after changing MWTM Security!!
```

```
[root@mwtm-server bin]# /opt/CSCOsgrm/bin/mwtm adduser newuser
Adding user newuser
New password:
Re-enter new password:
Adding password for user newuser
```

```
Should user be forced to change this password at the next login? [n] n
```

```
Access Level
=====
```

```
1 - Basic User
2 - Power User
3 - Network Operator
4 - Network Administrator
5 - System Administrator
```

```
Enter access level for user newuser: 5
User newuser added with level 5 access.
```

```
User Based Access Protection is Enabled.
```

```
Clear browser cache and restart browser after changing MWTM Security.
```

```
[root@mwtm-server bin]#
```

- Step 4** Make sure you restart the MWTM server (using the **mwtm restart** command) to activate the new security settings.
- 

**I'm field testing MWTM in my lab and I see confusing results when discovering new network configurations. What's going on?**

The MWTM keeps information about older objects in its database even after they have been deleted. This is considered a logically deleted state. MWTM retains this information to try and maintain any user customized data associated with an object (for instance, a customized name) in case the object is rediscovered at some point in the future. Logically deleted data is physically deleted after seven days if it is not reused by then. You can use the `mwtm purgedb` command to immediately remove this logically deleted data from the MWTM database.

Unfortunately, this benefit may have a side effect. In certain cases, rediscovery of a deleted object may cause the MWTM to use obsolete information in the database, rather than the new information. Ultimately, some configuration changes are not detected, and the viewable data from the client application is incorrect.

There are 2 alternatives to address this behavior in a lab environment:

1. Change the default setting of 7 days to 0 in the `Server.properties` file (using the `DELETE_AGING_TIMEOUT` variable).
2. Issue the “`mwtm purgedb`” command to immediately remove this logically deleted data from the MWTM database (for details, see [mwtm purgedb](#), page B-51).

# ITP Specific FAQs

This section addresses frequently asked questions related to ITP operations:

- [Can ITPs send traps to the MWTM and to another process on the same node?, page C-13](#)
- [Why did the MWTM not discover all of my ITP nodes?, page C-13](#)
- [How can the Received Utilization for some of my links be 105%?, page C-14](#)
- [What does the asterisk \(\\*\) mean next to an SLC number?, page C-14](#)
- [When I try to deploy routes, GTT files, or address table files from the MWTM, why does TFTP fail or time out?, page C-14](#)
- [Why don't my linkset and link totals match?, page C-14](#)
- [How do I enable accounting collection in the MWTM?, page C-14](#)
- [How do I generate custom ITP reports quarter hourly instead of hourly or daily?, page C-16](#)
- [Why do I have limited functionality on certain tabs?, page C-17](#)

## Can ITPs send traps to the MWTM and to another process on the same node?

Yes. You can configure your ITPs to send SNMP traps to more than one process on a single node. Each process receives traps on a different port number. However, to do so, you must configure a different community string for each process.

For example, your ITP configurations could include these lines:

```
snmp-server host 1.2.3.4 public udp-port 162
snmp-server host 1.2.3.4 otherCommunity udp-port 44750
```

where:

- The first line configures the HP OpenView trap receiver, with community string **public** and UDP port number **162**.
- The second line configures the MWTM trap receiver, with community string **otherCommunity** and UDP port number **44750**.

You would then configure the MWTM to receive traps on port number 44740. For information about how to configure the MWTM port number, see [Enabling SNMP Traps, page 3-7](#).

## Why did the MWTM not discover all of my ITP nodes?

After you discover the network, examine the Discovered Nodes table to verify that the MWTM discovered all of the nodes in the network. If you suspect that the MWTM did not discover all of the nodes, verify these conditions:

- Verify that the MWTM server can ping the nodes.
- Verify that the nodes are running ITP IOS images that are compatible with the MWTM server.
- Verify that the SNMP is enabled on the nodes.
- Verify that the MWTM is configured with the correct SNMP community name (see [Launching the Discovery Dialog, page 4-6](#)).
- Verify that the missing nodes are connected to the seed nodes by SCTP connections, not just serial connections.
- Verify that you chose **Entire Network** when you ran Discovery. If you suspect that you did not, run Discovery again with **Entire Network** chosen.

**How can the Received Utilization for some of my links be 105%?**

For serial and HSL links on Cisco 7507 and 7513 series routers, in the Received Utilization and Send Utilization real-time data charts for links and linksets, the visible utilization data can vary by up to 5% from the actual utilization—the MWTM might even display utilization data above 100%. This variance results from the synchronization of Layer 2 counters between the Versatile Interface Processor (VIP) CPU and the Route Switch Processor (RSP) CPU on 7500 series routers. This variance does not occur for links on Cisco 2600, 7200, or 7300 series routers.

**What does the asterisk (\*) mean next to an SLC number?**

In the MWTM, each link is identified by its signaling link code ID (SLC). An asterisk indicates that a link is not configured, or that a poll could not get data for the link.

The placement of the asterisk, to the left or right of the SLC, indicates whether the missing link is associated with the chosen linkset or with its adjacent linkset. For example, **SLC (\*)3** means that no link is associated with the chosen linkset for SLC 3, and **SLC 3(\*)** means that no link is associated with the adjacent linkset for SLC 3.

**When I try to deploy routes, GTT files, or address table files from the MWTM, why does TFTP fail or time out?**

There are three primary causes for TFTP failure or timeout errors:

- You might not have enabled TFTP on your server, which will cause a timeout error (see [Setting Up TFTP on Your Server \(ITP Only\)](#), page 3-12).
- You might have specified your tftp root directory (by default, /tftpboot) in the tftp path, which is not necessary and will cause TFTP to fail. For details on specifying the correct path, see these sections:  
[mwtm atbldir](#), page B-90  
[mwtm gttdir](#), page B-98  
[mwtm routedir](#), page B-114
- If the staging directory (created using the previous commands) does not have write permissions for the MWTM server processes, the TFTP will fail.

**Why don't my linkset and link totals match?**

When you run the **mwtm export** command for a link or linkset, you might notice the output totals do not match the totals in the MWTM client. This discrepancy occurs because the **mwtm export** command counts each side of the linkset or link as a individual linkset or link, whereas the MWTM client (assuming it knows both sides) counts both sides as one linkset or link pair. Therefore, the **mwtm export** command might have more linksets and links than the MWTM client shows.

**How do I enable accounting collection in the MWTM?**

Enabling accounting collection in the MWTM is described next. First, you must enable accounting on each ITP node using IOS commands. Then you can enable accounting in the MWTM.

**Note**

Enable accounting on each ITP node using IOS commands. Accounting can be enabled on the ITP globally or per linkset. For detailed information on IOS modes and commands, see the Cisco IOS software documentation.

To enable accounting globally for all linksets on an ITP node:

**Step 1** Go into IOS global configuration (**configure terminal**) mode.

**Step 2** Enter these commands and arguments:

```
node name(config)#cs7 accounting global-gtt
node name(config)#cs7 accounting global-mtp3
node name(config)#cs7 accounting global-unrouteable
```



**Note** These IOS arguments are the recommended defaults for the MWTM.

To enable accounting per linkset on an ITP node:

**Step 1** Go into IOS global configuration (**configure terminal**) mode.

**Step 2** Enter these commands and arguments:

```
node name(config)#cs7 instance number linkset name
node name(config)#accounting
node name(config)#gtt-accounting
node name(config)#unrouteable-accounting
```



**Note** These arguments are the recommended defaults for the MWTM. The instance number argument is not required if you have only one instance.

The MWTM accounting reports are disabled by default. Enable them:

**Step 1** Enter these commands:

```
node name#/opt/CSCOsgm/bin/sgm statreps acct
node name#/opt/CSCOsgm/bin/sgm statreps gtt
```

Data is collected daily, and is not affected by polling interval preferences in the Java or web clients.



**Note** These arguments are the recommended defaults for the MWTM. However, other arguments are available. For a full list of **mwtm statreps** commands, see [Appendix B, “Command Reference.”](#)

**Step 2** Polling intervals for historical reports are controlled by the root user’s crontab file. To display the current values for crontab, and to verify that accounting reports are enabled, run this command:

```
node name#crontab -l
```

The list should include **statreps acct** and **statreps gtt**.

### How do I generate custom ITP reports quarter hourly instead of hourly or daily?

You can manually generate custom reports using the MWTM command line interface (CLI). These commands apply to generating custom reports:

- `mwtm accstats quiet`
- `mwtm gttstats quiet`
- `mwtm linkstats quiet`
- `mwtm mlrstats quiet`
- `mwtm q752stats quiet`
- `mwtm xuastats quiet`

The quiet option disables output to the console.

The output of these commands is placed in this directory:

`/opt/CSCOsgm/reports/custom`



#### Note

For details on these commands, see [Appendix B, “Command Reference.”](#)

Use the UNIX cron facility to schedule the CLI commands to be run every quarter hour:

**Step 1** Log in as the root user, as described in [Becoming the Root User \(Server Only\)](#), page 4-2.

**Step 2** Enter this command to edit the crontab:

```
crontab -e
```

**Step 3** For example, if you wanted to have the link and XUA statistic reports run every quarter hour instead of hourly or daily:

a. Comment out these lines:

```
54 * * * * /opt/CSCOsgm/bin/sgmCron.sh xuastats
56 * * * * /opt/CSCOsgm/bin/sgmCron.sh linkstats
```

b. Add a line similar to these for each report command:

```
00,15,30,45 * * * * /opt/CSCOsgm/bin/mwtm linkstats quiet
00,15,30,45 * * * * /opt/CSCOsgm/bin/mwtm xuastats quiet
```

You can find these reports in this directory:

`/opt/CSCOsgm/reports/custom`

There will be 15 minute timestamps on each report file.

**Step 4** To view these reports on the web, open the MWTM web interface (see [Accessing the MWTM Web Interface](#), page 11-1) then choose **File Archive > Reports > Custom**.



#### Note

You can keep both the standard hourly reports and the 15 minute reports by leaving both types in the crontab instead of commenting out the lines in the previous steps. This will generate a heavier load on the system for a few minutes at the top of the hour when both are running at the same time.

**Why do I have limited functionality on certain tabs?**

You might notice limited functionality on the following ITP tabs:

- MSU Rates
- MLR Details
- Non-Stop Operation

These tabs are available on certain nodes, and also require specific IOS images:

| Tab                | Node Availability                    | IOS Required Images                                                                                                                           |
|--------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| MSU Rates          | All                                  | <ul style="list-style-type: none"> <li>• 12.2 (18) IXB or later</li> <li>• 12.2 (25) SW7 or later</li> <li>• 12.4 (11) SW or later</li> </ul> |
| MLR Details        | All                                  | <ul style="list-style-type: none"> <li>• 12.2(18)IXA or later</li> <li>• 12.2(21)SW1 or later</li> <li>• 12.4(11)SW or later</li> </ul>       |
| Non-Stop Operation | Cisco 7500 and Cisco 7600 nodes only | <ul style="list-style-type: none"> <li>• 12.2 (18) IXA or later</li> <li>• 12.2(21)SW or later</li> <li>• 12.2 (4)MB13a or later</li> </ul>   |

## RAN-O Specific FAQs

This section addresses frequently asked questions related to RAN-O operations:

- [What is the difference between in-band and out-of-band management?, page C-18](#)
- [How does the MWTM server communicate to the RAN-O node at the remote cell site?, page C-19](#)
- [When viewing capacity planning information in the RAN Backhaul Utilization report, the peak timestamps are sometimes outside the chosen range. For example, 2005-12-01 appears in the report window, but I see Nov 30, 2005 11:58:37 PM in the Peak Timestamp information. Why is the peak timestamp outside the chosen range?, page C-20](#)
- [Does the MWTM support the use of Hot Standby Router Protocol \(HSRP\) for a pair of redundant nodes?, page C-20](#)
- [How do I sync up the time/date display on my RAN-O performance and error data with the time/date on the MWR?, page C-20](#)
- [Why are my MWR nodes yellow when I discover them?, page C-22](#)
- [Why does my backhaul utilization graph show greater than 100% for transmit traffic?, page C-22](#)

### What is the difference between in-band and out-of-band management?

Nodes located at the cell site are usually accessible only over the same path used to transport voice traffic. Collecting management information over this path is called in-band management and has an impact on backhaul utilization. The MWTM can reduce the amount and frequency of collecting management information when information is collected in-band.

Nodes located at the aggregation site are managed using different paths than those used by voice traffic. Collecting management information in this configuration is called out-of-band management and has no impact on backhaul utilization.

The following table compares MWTM features for in-band and out-of-band management:

| Feature                      | In-band Management for MWR   | Out-of-band Management for MWR |
|------------------------------|------------------------------|--------------------------------|
| Historical reports           | Not available <sup>1</sup>   | Generated                      |
| Trap polling                 | Traps do not trigger polling | Traps do trigger polling       |
| Regular polling <sup>2</sup> | Performed                    | Performed                      |
| Real-time polling            | Available <sup>3</sup>       | Performed                      |

1. However, you can always collect historical reports from the agg node site (ie, the RAN SVC module in the ONS). The receiving traffic on the RAN SVC shorthaul and backhaul matches transmitting traffic from the MWR shorthaul and backhaul.
2. Polls are performed every 15 minutes. To change this rate, see the SNMP and Credentials Dialog Box (for details, see [SNMP Settings Table, page 3-16](#)).
3. To perform real-time polling in-band, you must configure it in the Preferences window (for details, see [Startup/Exit Settings, page 5-4](#)).

- These cell-site node configuration statements provide the MWTM with information required to optimize data collection:

```
conf t
 ipran-mib location cellSite
 ipran-mib snmp-access inBand
```

- If you have a cell-site node that is managed out-of-band, or you have sufficient bandwidth for in-band managed traffic, you can configure the cell-site node as follows:

```
conf t
 ipran-mib location cellSite
 ipran-mib snmp-access outOfBand
```

- These aggregation-site node configuration statements provide the MWTM with information required to optimize data collection:

```
conf t
 ipran-mib location aggSite
 ipran-mib snmp-access outOfBand
```

This example shows the range of options that are available for the **ipran-mib** command:

```
ems1941ka#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ems1941ka(config)#ipran-mib ?
 backhaul-notify-interval Interval for backhaul utilization
 location Location of device
 snmp-access Specify type snmp connectivity
 threshold-acceptable Acceptable utilization threshold
 threshold-overloaded Overloaded utilization threshold
 threshold-warning Warning utilization threshold
```



```

ems1941ka(config)#ipran-mib location ?
aggSite Located at BSC or RNC site
cellSite Located at BTS or Node B site
undefined Undefined location

ems1941ka(config)#ipran-mib snmp-access ?
inBand In Band SNMP connectivity
outOfBand Out of Band SNMP connectivity
undefined Undefined connectivity

```

#### How does the MWTM server communicate to the RAN-O node at the remote cell site?

The MWTM server must communicate to the cell-site node using IP routing. If the cell-site node is reachable only through the backhaul interface, add a static route on the MWTM server to point to the cell-site node. Use the IP address of the local (aggregation site) RAN-O node as the next-hop address.

These examples of static routing for Solaris and Linux platforms are based on the diagram in [Figure C-2](#).

**Figure C-1** Example of Static Routing

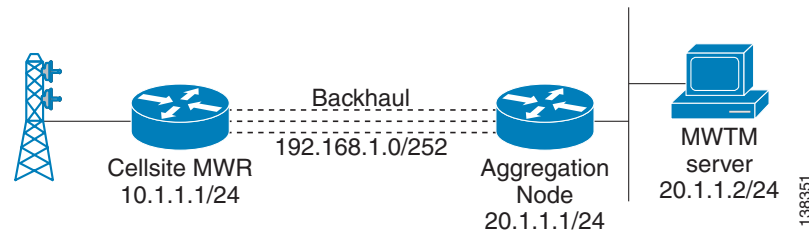
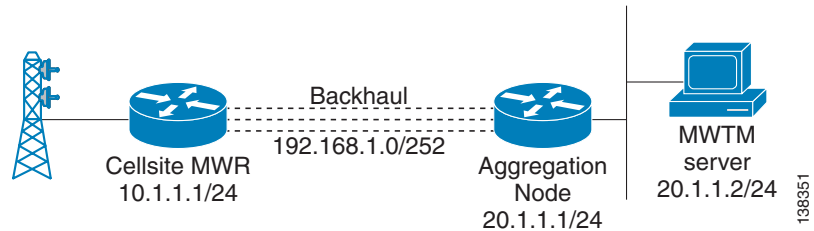


**Figure C-2** Example of Static Routing



To create a static route on a Solaris MWTM server, use this procedure:

---

**Step 1** Log in as the root user, as described in [Becoming the Root User \(Server Only\)](#), page 4-2.

**Step 2** Enter this command:

```
/usr/sbin/route add host 10.1.1.1 20.1.1.1
```

---

To create a static route on a Linux MWTM server, use this procedure:

---

**Step 1** Log in as the root user, as described in [Becoming the Root User \(Server Only\)](#), page 4-2.

**Step 2** Enter this command:

```
route add -host 10.1.1.1 gw 20.1.1.1
```

**When viewing capacity planning information in the RAN Backhaul Utilization report, the peak timestamps are sometimes outside the chosen range. For example, 2005-12-01 appears in the report window, but I see Nov 30, 2005 11:58:37 PM in the Peak Timestamp information. Why is the peak timestamp outside the chosen range?**

Summaries do not end on fifteen-minute boundaries such as 12:00:00, 12:15:00, 12:30:00, because the node processes system time from its own start time, not from the current hour and minute. Therefore, when the timestamps are normalized to the MWTM server time, the end timestamp might appear as 12:03:15, 12:18:15, or 12:33:15.

When you run a capacity planning report, the MWTM retrieves records for the fifteen-minute period that has an end timestamp in the start and stop range that you specify. Using the previous timestamps as examples, if a user runs a report for the 12:00-to-13:00 time range, the 12:03:15 record is retrieved. That record is a fifteen-minute summary of the period between 11:48:16 and 12:03:15. If the Peak Timestamp for this record occurred at 11:55:44, the user would observe this value in the capacity planning report.

A user might observe Peak Timestamps that occur up to fifteen minutes before the start timestamp specified in the capacity planning report query. This is the expected behavior.

**Does the MWTM support the use of Hot Standby Router Protocol (HSRP) for a pair of redundant nodes?**

The MWTM supports HSRP for the Cisco Mobile Wireless Router (MWR) 1941-DC-A operating in an active-standby configuration. The MWTM supports these scenarios:

- An MWR fails at the cell site, and you install a new MWR to replace it. The MWTM applies the same IP address and configuration to the new MWR, but shows a different serial number. The MWTM detects that the new MWR is at the same cell site as the old MWR, and reuses the historical statistics for this node.
- You deploy two MWRs as a redundant pair by using the Y-cable configuration described in the [Cisco MWR 1941-DC-A Mobile Wireless Edge Router Software Configuration Guide](#). When a failover occurs, the MWTM detects that the newly active node is at the same cell site as the standby node. The MWTM reuses the historical statistics for this node.
- The MWTM shows a failover alarm or a series of events associated with the failover between the active and standby nodes in a redundant pair of MWRs.



**Note** The MWTM GUI shows only the active MWR in an active-standby pair.

Because the IOS configs are not synchronized between MWR nodes, make sure the IOS configs are identical (except HSRP settings) on both nodes.

**How do I sync up the time/date display on my RAN-O performance and error data with the time/date on the MWR?**

For the performance and error data to match the time/date on the MWRs, all equipment (Cisco and MWTM server) must be configured with the same Network Time Protocol (NTP) server.

To configure NTP on the Cisco node:

**Step 1** Log in to the node.

**Step 2** Go into config mode.

- Step 3** Enter:
- ```
ntp server <ip-address-of-ntp-server>
```
- Step 4** Exit the config mode
- Step 5** Save the configuration.

To configure NTP on a Solaris-based MWTM server:

- Step 1** Log in as the root user.
- Step 2** Edit the */etc/ntp.conf* file by adding this line:
- ```
server <ip-address-of-ntp-server>
```
- Step 3** Restart the NTP software using this command:
- ```
/etc/init.d/ntpd restart
```
- Step 4** Run the date command and ensure the clock has been set properly.
- If the date is still incorrect, follow these instructions:
- Stop the NTP software using the following command:
- ```
/etc/init.d/ntpd stop
```
- Manually sync the date using the following command:
- ```
/usr/sbin/ntpdate <ip-address-of-ntp-server>
```
- Start the NTP software using the following command:
- ```
/etc/init.d/ntp start
```



**Note** To enable the NTP software, the packages SUNWntpr and SUNWntpu are required. As the root user, run the command: **pkginfo | grep SUNWntp**. You can download missing packages from Sunfreeware.com.

To configure NTP on a Linux-based server:

- Step 1** Log in as the root user
- Step 2** Edit the *ntp.conf* file (usually located in */etc*, */etc/inet*, or */etc/ntp/ntpervers*) by adding the following line:
- ```
server <ip-address-of-ntp-server>
```
- Step 3** Restart the NTP software using this command:
- ```
/etc/init.d/ntpd restart
```

**Step 4** Run the date command and ensure the clock has been set properly.

If the date is still incorrect, follow these instructions:

- a. Stop the NTP software using the following command:

```
/etc/init.d/ntp stop
```

- b. Manually sync the date using the following command:

```
/usr/sbin/ntpdate <ip-address-of-ntp-server>
```

- c. Start the NTP software using the following command:

```
/etc/init.d/ntp start
```



**Note** The NTP package is required to enable the NTP software. To determine if the NTP package has been installed, run the command **rpm -qa | grep -i ntp** as the root user. Missing packages can be downloaded from RPMFind.net.

### Why are my MWR nodes yellow when I discover them?

When the MWTM discovers or polls a node, a list of all interfaces and their corresponding status are reported back to the MWTM server. If the MWTM determines that one or more interfaces are operationally down, the MWR node is marked with a yellow status symbol unless the interface has an administrative status of Down (coming from the IOS shutdown directive). To determine the status of an interface, the MWTM uses the following logic matrix:

| Interface Admin Status | Interface Operational Status | Reported Interface Status | MWTM Ignored Status |
|------------------------|------------------------------|---------------------------|---------------------|
| Up                     | Up                           | Up                        | Not ignored         |
| Up                     | Down                         | Down                      | Not ignored         |
| Down                   | Down                         | Down                      | Ignored             |
| Down                   | Up                           | Down                      | Ignored             |



**Note** As shown in the above matrix, MWTM automatically ignores any interface with an administrative status of Down.

### Why does my backhaul utilization graph show greater than 100% for transmit traffic?

When the backhaul utilization for transmit traffic exceeds 100%, the likely cause is oversubscription of the shorthaul links that constitute the backhaul. The backhaul utilization is the amount of traffic that the system attempted to send, not the amount that was actually sent. If utilization is greater than 100%, you should see queue drops or other errors during the same time period. A backhaul utilization of greater than 100% is possible for a heavily loaded link with some occasional oversubscription.



## APPENDIX **D**

# Troubleshooting the MWTM and the Network

---

This chapter provides this information for troubleshooting basic Cisco Mobile Wireless Transport Manager (MWTM) network problems:

- [Clearing a Locked-Up MWTM Display, page D-1](#)
- [Investigating Data Problems, page D-1](#)
- [Understanding MWTM Client Start Error Messages, page D-2](#)
- [Checking MWTM Server Start Processes, page D-3](#)
- [Viewing the MWTM Troubleshooting Log, page D-3](#)
- [Viewing MWTM Data on the Web, page D-4](#)
- [Troubleshooting IOS Commands on the Web, page D-4](#)
- [Viewing Detailed Troubleshooting Instructions for Events, page D-5](#)
- [Diagnosing a Typical Network Problem, page D-5](#)

## Clearing a Locked-Up MWTM Display

In the MWTM, events might cause message popups to remain in the background of your display, preventing you from interacting with other windows. If you suspect that your display has locked up, perform these tasks:

- Ensure that you are running the MWTM on a supported operating system. For details on supported operating systems, see Chapter 1, “Preparing to Install the MWTM” in the *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.1*.
- Minimize windows and look for an MWTM message popup in the background.

## Investigating Data Problems

If you suspect that there are problems with the data that the MWTM is displaying, perform these tasks:

- Enter equivalent **show** commands on the router. Is the data the same as that visible by the MWTM?
- Send SNMP queries to the nodes. Do all queries complete?

The results of these tasks can help you distinguish between a router problem and an MWTM problem.

# Understanding MWTM Client Start Error Messages

If you encounter one of these errors upon starting the MWTM client, follow the subsequent procedures:

- DataModelMediatorService: Could not find service in RMI registry or the RMI Registry may be down.
- DemandPollerManagerService: Could not find service in RMI registry or the RMI registry may be down. Check the MWTM server and ensure that it is running.

## Data Model Mediator Service Error

If you have received this message: “DataModelMediatorService: Could not find service in RMI registry or the RMI Registry may be down” either you have specified an incorrect port number when installing the MWTM, or the server or RMI registry is unavailable.

To correct this problem:

|        |                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | Verify that you specified a correct port number.                                                                  |
| Step 2 | Enter the <b>mwtm status</b> command on the server to determine the status of all MWTM servers on the local host. |
| Step 3 | Enter the <b>mwtm restart</b> command to restart any servers that are not running.                                |

## Demand Poller Manager Service Error

If you have received this message: “DemandPollerManagerService: Could not find service in RMI registry or the RMI registry may be down. Check the MWTM server and ensure that it is running” one or more of the MWTM server processes may not have started.

To diagnose and correct this problem:

Step 1

Enter the **mwtm status** command on the server to determine the status of all MWTM processes.

Check the output to see if the sgmDataServer and sgmTrapReceiver processes do not appear in the Ready state. They may appear:

| PROCESS         | STATE    | PID  | Last Message                       |
|-----------------|----------|------|------------------------------------|
| sgmDataServer   | Starting | 2586 | Starting EventModelMediatorService |
| sgmMsgLogServer | Ready    | 2551 | Running                            |
| sgmTrapReceiver | Initial  |      |                                    |

Step 2

If the processes are not all in a Ready state, search log file */opt/CSCOsgm/logs/messageLog.txt* for this error message:

A java.IO.EOFException was encountered against the persisted.server.data file.

- Step 3** Enter the **mwtm cleandb** command on the server, which will restore the *persisted.server.data* file to a valid state. The output should now show all processes running:

| PROCESS         | STATE | PID  | Last Message |
|-----------------|-------|------|--------------|
| sgmDataServer   | Ready | 2586 | Running      |
| sgmMsgLogServer | Ready | 2551 | Running      |
| sgmTrapReceiver | Ready | 2600 | Running      |

- Step 4** Start the MWTM client, then re-discover the network (for details, see [Discovering Your Network, page 4-4](#).)

## Checking MWTM Server Start Processes

When you run the **mwtm start** command, normal output appears:

| PROCESS         | STATE | PID  | Last Message |
|-----------------|-------|------|--------------|
| sgmDataServer   | Ready | 2586 | Running      |
| sgmMsgLogServer | Ready | 2551 | Running      |
| sgmTrapReceiver | Ready | 2600 | Running      |

If the sgmDataServer and sgmTrapReceiver process do not appear in the Ready state, see [Demand Poller Manager Service Error, page D-2](#) for details on fixing this issue.

## Viewing the MWTM Troubleshooting Log

The MWTM stores troubleshooting information in the */opt/CSCOsgm/tmp/cisco\_sgm\_tshoot.log* file on the MWTM server. This log, which is updated each time the MWTM Server Troubleshooting page is accessed or the **mwtm tac** command is run, contains information that might be requested by Cisco customer support personnel.

To view the log from the command line:

- Step 1** Log in as the root user, as described in [Starting the MWTM Client, page 4-2](#), or as a superuser, as described in [Specifying a Super User \(Server Only\), page 2-20](#).

- Step 2** Enter:

```
cd /opt/CSCOsgm/bin
./mwtm tac
```

This command might take a minute or more to complete. When it completes, the MWTM shows this message and prompt:

```
Output is in /opt/CSCOsgm/tmp/cisco_sgm_tshoot.log
Would you like to view it? [y]
```

- Step 3** Press **Enter**. The MWTM shows the contents of the */opt/CSCOsgm/tmp/cisco\_sgm\_tshoot.log* file.

# Viewing MWTM Data on the Web

The MWTM provides an enormous amount of web-based troubleshooting information. From the MWTM web interface, you can access many web pages containing MWTM data, including server status, network status, installation logs, message logs, product documentation, and other important troubleshooting information about the MWTM. For full details, see [Chapter 11, “Accessing Data from the Web Interface.”](#)

## Troubleshooting IOS Commands on the Web



**Note**

If you have implemented MWTM User-Based Access, this option is available to users with authentication level Network Operator (level 3) and higher.

You can perform troubleshooting on a node or an object in the node’s hierarchy by:

1. Selecting an object in a view in the navigation tree
2. Clicking the Troubleshooting tab in the right pane



**Note**

The Troubleshooting tab is not available for all objects in the navigation tree.



**Tip**

To save the output of all executed commands to a log file, see [mwtm tshootlog, page B-77](#).

Before you can run commands and view output, credentials must be properly configured. You can configure credentials using the CLI command (see [mwtm addcreds, page B-6](#)) or through the MWTM client (see [Configuring Login Credentials, page 3-20](#)). If credentials are not configured, the message “No credentials available. Add credentials and reload the page” appears in the output pane.

The right pane for the Troubleshooting table shows these fields and toolbar buttons for the chosen object:

| Field or Toolbar Button         | Description                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Name<br>(in heading)     | Name as discovered by the MWTM.                                                                                                                              |
| Server Name<br>(in heading)     | Name of the MWTM server associated with the node.                                                                                                            |
| Update Interval<br>(in heading) | Time between automatic updates for the page.                                                                                                                 |
| Last Update<br>(in heading)     | Date and time the information on the page was last updated by the MWTM.                                                                                      |
| Category                        | Related commands are grouped together in categories. Some categories are provided by default and cannot be modified. Additional categories are user-defined. |
| Command                         | List of commands or tasks associated with the chosen category. A chosen command can be executed using the <b>Execute Command</b> button.                     |



| Field or Toolbar Button                                                                            | Description                                   |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------|
|  Execute Command  | Executes the chosen command only.             |
|  Execute Category | Executes all commands in the chosen category. |
|  Cancel Execution | Stops any execution process.                  |
|  Clear Output     | Clears all output from the screen.            |
| Output Pane                                                                                        | Pane at bottom where command output appears.  |

**Related Topics**

- [Configuring Login Credentials, page 3-20](#)
- [Viewing Troubleshooting, page 8-43](#)
- [mwtm addcreds, page B-6](#)
- [mwtm tshootlog, page B-77](#)

## Viewing Detailed Troubleshooting Instructions for Events

The MWTM provides extensive type-specific help and troubleshooting instructions for events. To see help and troubleshooting instructions for an event, right-click the event and select **Help for Event**.

You can also provide your own enterprise-specific instructions to operators in the event help. For more information, see [Changing the Way the MWTM Processes Events, page 9-35](#).

## Diagnosing a Typical Network Problem

This section contains this content:

- [Diagnosing a Typical ITP Network Problem, page D-6](#)
- [Diagnosing a Typical RAN-O Network Problem, page D-8](#)

When you use the MWTM to diagnose a problem in a network, follow these basic steps:

- 
- |               |                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Monitor the network using the MWTM main window and the topology window. For example, an object in the topology map that changes color from green to yellow or red indicates a problem in the network. |
| <b>Step 2</b> | Use MWTM windows, especially the Details window, to begin investigating the problem.                                                                                                                  |
| <b>Step 3</b> | As you identify the source of the problem, examine the messages logged by the MWTM for more detailed information about the sequence of events that led to the problem.                                |
| <b>Step 4</b> | Connect (by using Telnet or SSH) to the problematic node, if necessary.                                                                                                                               |
-

## Diagnosing a Typical ITP Network Problem

This real-life example provides detailed information about using the MWTM to diagnose a problem in an ITP network:

- 
- Step 1** A network operator (we'll call him Joe) is using the MWTM to monitor an ITP network. Joe has customized his view, limiting it to only those nodes for which he is responsible.
- (For more information about customizing views, see [Chapter 7, "Managing Views."](#))
- Step 2** In the topology map, Joe notices a signaling point that has changed color from green to yellow. Yellow indicates a status of Warning, which means that one or more links or linksets associated with that signaling point is in Unknown or Warning status and is not flagged as Ignored.
- (For more information about signaling point status, see [Viewing Details, page 8-12.](#))
- Step 3** Joe single-clicks the signaling point in the topology map.
- The MWTM highlights the signaling point in the topology map, and in the topology ASP/SP/view table, in the left pane of the topology window. With the signaling point highlighted, Joe can easily see that the name of the signaling point is sgm-7500j.
- The MWTM also shows all associated linksets in the topology ASPA/linkset table.
- Joe double-clicks the signaling point's name in the topology ASP/SP/view table.
- The MWTM redraws the topology map, centered on sgm-7500j, making it easier for Joe to see the relevant portion of the map.
- (For more information about the topology window and how to use it, see [Chapter 10, "Viewing Network Topology."](#))
- Step 4** Joe notices that one of sgm-7500j's diamonds is red, indicating that the associated linkset is either Unavailable or Unknown. Joe single-clicks the red diamond.
- The MWTM highlights the linkset in the topology map and in the topology ASPA/linkset table. The table entry indicates that the linkset is Unavailable.
- (For more information about linkset status, see [Viewing Details, page 8-12.](#))
- Step 5** Joe right-clicks the linkset in the topology map and selects **View > Details** in the right-click menu.
- The MWTM opens the Details window, showing detailed information for the linkset.
- In the Details window, detailed information for the chosen linkset appears in the left column and for the adjacent linkset in the right column
- Immediately, Joe sees that the left column is populated with MWTM data, but the right column is not. The problem is in the adjacent signaling point-to-primary signaling point linkset.
- (For more information about linkset details, see [Chapter 8, "Understanding Detailed Object Functions."](#))
- Step 6** Joe clicks on Linkset under Summary Lists to display the list of links associated with the linkset, identified by their signaling link code IDs (SLCs). In this case, only one link is listed, SLC 0, and it is red, meaning it has failed and no traffic is flowing on the link.
- Joe selects SLC 0, and the MWTM shows detailed information for the link in the left column. Normally the MWTM also shows detailed information for links associated with the adjacent linkset in the right column, but in this case, that column is blank.
- (For more information about linkset status, see [Viewing Details, page 8-12.](#))

- Step 7** Joe decides to investigate the adjacent signaling point, so he double-clicks the adjacent signaling point in the topology map.
- The resulting display shows that the adjacent signaling point, sgm-2600a, is Unmanaged.
- (For more information about signaling point details, see [Chapter 8, “Understanding Detailed Object Functions.”](#))
- Step 8** Joe closes the Details window and returns to the topology window. He tries to find sgm-2600a in the topology map, but the map is too complex. So Joe lets the MWTM find the signaling point or application server process for him:
- He selects **Edit > Find** in the MWTM main menu. The Find dialog box appears.
  - He enters sgm-2600a in the Search string field and makes sure the Name, check box is checked.
  - He clicks **OK** to launch the search. Almost immediately, the MWTM finds the signaling point or application server process and the Choose dialog box appears, listing all found objects.
  - Joe selects sgm-2600a, and the MWTM automatically highlights sgm-2600a in the topology ASP/SP/view table and in the topology map, and redraws the map centered on sgm-2600a.
- (For more information about finding objects in the topology map, see [Chapter 10, “Viewing Network Topology.”](#))
- Step 9** Joe wants to see recent events for sgm-2600a, so he clicks the signaling point in the topology map and selects **View > Events** in the MWTM main menu. The Recent Events tab appears for the chosen object, in this case showing recent events for sgm-2600a.
- (For more information about viewing events, see [Chapter 9, “Managing Alarms and Events.”](#))
- Step 10** Joe decides to see if the MWTM can manage the signaling point. He right-clicks sgm-2600a in the topology map and selects Manage in the right-click menu.
- The MWTM changes the status of the signaling point from Unmanaged (red) to Warning (yellow), which means the signaling point is active, but one or more associated linksets or links has a status of Failed, Unavailable, Unknown, or Warning and is not flagged as Ignored.
- (For more information, see [Unmanaging and Managing Nodes or ITP Signaling Points, page 6-42.](#))
- Step 11** Joe wants to see status change messages for sgm-2600a, so he right-clicks the signaling point again and selects **Event History > Status Change Messages** in the right-click menu. The MWTM shows recent status change messages for the signaling point in a web browser.
- Joe sees that many of the links and linksets associated with sgm-2600a have a status of Unknown.
- (For more information about displaying messages on the web, see [Chapter 11, “Accessing Data from the Web Interface.”](#))
- Step 12** At this point, Joe must determine why so many of the links and linksets are Unknown. He must verify that the MWTM server can ping the node (see [Enabling the Terminal Server Proxy Service, page 3-11](#)), and that the MWTM is configured with the correct SNMP community name for the node (see [Launching the Discovery Dialog, page 4-6](#)).
- (For a list of some other actions Joe can take, see [Verifying Discovery, page 4-15](#).)
- Step 13** Finally, Joe can use another product, such as CiscoView, to further investigate the problem.
- (For more information about integrating the MWTM with CiscoView and other products, see [Integrating the MWTM with Other Products, page 5-39](#).)
-

## Diagnosing a Typical RAN-O Network Problem

This real-life example provides detailed information about using the MWTM to diagnose a problem in a RAN-O network:

- 
- Step 1** A network operator (we'll call him Joe) is using the MWTM to monitor a RAN-O network. Joe has customized his view, limiting it to only those nodes for which he is responsible.
- (For more information about customizing views, see [Chapter 7, "Managing Views."](#))
- Step 2** In the topology map, Joe notices a node that has changed color from green to yellow. Yellow indicates a status of Warning, which means that one or more interfaces associated with that node is in Unknown or Warning status and is not flagged as Ignored.
- (For more information about node status, see the ["Viewing Details" section on page 8-12.](#))
- Step 3** Joe single-clicks the node in the topology map.
- The MWTM highlights the node in the topology map and in the topology view table in the left pane of the topology window. With the node highlighted, Joe can easily see that the name of the node is MWR-1941a.
- The MWTM also shows all associated interfaces in the topology Connections table.
- Joe clicks the node's name and the zoom button in the topology view table.
- The MWTM redraws the topology map, centered on MWR-1941a, making it easier for Joe to see the relevant portion of the map.
- (For more information about the topology window and how to use it, see [Chapter 10, "Viewing Network Topology."](#))
- Step 4** Joe notices that one of MWR-1941a's diamonds is red, indicating that the associated interface is either Unavailable or Unknown. Joe single-clicks the red diamond.
- The MWTM highlights the connection in the topology map and in the topology Connections table. The table entry indicates that the connection is Unavailable.
- Step 5** Joe right-clicks the connection in the topology map and selects **View > Configuration Details** in the right-click menu.
- The MWTM opens the Details window (in the main MWTM window), showing detailed information for the connection. In the Details window, detailed information for the chosen connection appears in the Configuration Data section.
- Immediately, Joe sees that the Operational Status is Down but notices that the Operational Status for E1 1/0 is Up.
- Step 6** Joe selects the Recent Events tab and notices that a Critical Alarm for E1 1/0 was recently added.
- Joe logs into the MWR-1941a node (right-click on node name and choose **Node > Connect To**) and runs the **show controller E1 1/0** command. He learns that the node recently loss physical connectivity.
- Step 7** Joe goes to the router and discovers that the cable is physically damaged. He replaces the cable and returns to the MWTM server.
- Step 8** Joe views the MWTM main window and observes that the MWTM has already polled the node and changed the state color from yellow to green.
- Step 9** Joe looks at the MWTM topology window again and verifies the interface status has changed from yellow to green.
-



# APPENDIX **E**

## Status Definitions

---

This appendix defines the default status settings for all Cisco Mobile Wireless Transport Manager (MWTM) network objects.

This appendix contains:

- [General Status Definitions, page E-1](#)
- [ITP Status Definitions, page E-3](#)
- [RAN-O Status Definitions, page E-7](#)
- [mSEF Status Definitions, page E-10](#)

## General Status Definitions

The following status definitions apply to both ITP, IPRAN, and mSEF networks:

- [Status Definitions for Nodes, page E-1](#)
- [Status Definitions for Views, page E-2](#)
- [Status Definitions for Folders, page E-2](#)
- [Status Definitions for Interfaces, page E-2](#)

## Status Definitions for Nodes

Possible values for the current status of the node are:

-  **Active**—The node is currently fully functional.
-  **Discovering**—The node is being discovered, and Simple Network Management Protocol (SNMP) queries have been sent to the node.
-  **Polling**—The node is being polled.
-  **Unknown**—The node failed to respond to an SNMP request. The MWTM sets all associated signaling points, linksets, or links to Unknown.

-  **Unmanaged**—One of these situations exists:
  - The node is known indirectly by the MWTM. In other words, the MWTM knows the node exists but there is no known SNMP stack on the node for the MWTM to query.
  - An MWTM user has set the node to Unmanaged status, to prevent the MWTM from polling the node.

(ITP only) If the associated signaling points are referenced via linksets to other signaling points, the MWTM automatically sets all associated signaling points to Unmanaged, and deletes all associated linksets and links, as well as all linksets and links that reference the node as an adjacent node.

(ITP only) If the associated signaling points are not referenced to other signaling points, the MWTM automatically deletes the signaling points, all associated linksets and links, and all linksets and links that reference the node as an adjacent node.
-  **Waiting**—The node is in the Discovery queue but is not currently being discovered.
-  **Warning**—The node is active, but one or more associated objects are in Failed, Unavailable, Unknown, or Warning status and are not Ignored.

## Status Definitions for Views

Possible values for the current status of the view are:

-  **Active**—All objects in the chosen view are currently Active and fully functional.
-  **Unmanaged**—All objects in the chosen view are currently Unmanaged.
-  **Warning**—One or more objects in the chosen view is currently not Active.

## Status Definitions for Folders

Possible values for folders (such as Physical and Mgmt Interfaces) are:

-  **Active**—All objects in the chosen folder are currently Active and fully functional.
-  **Warning**—At least one object is not Active.

## Status Definitions for Interfaces

This section provides definitions for these statuses:

- [Admin Status, page E-2](#)
- [Operational Status, page E-3](#)
- [Status, page E-3](#)

### Admin Status

Possible values for the administrative status of the interface are:

-  **Unknown**—Unknown administrative status
-  **Up**—Administratively up

-  **Shutdown**—Administratively down
-  **Testing**—Administrator is testing the interface

## Operational Status

Possible values for the operational status of the interface are:

-  **Unknown**—Unknown operational status.
-  **Up**—Interface is up.
-  **Down**—Interface is down.
-  **Testing**—Interface is in test mode.
-  **Dormant**—Interface is dormant.
-  **Not Present**—An interface component is missing.
-  **Lower Layer Down**—An interface is down because of a lower-layer interface.

## Status

Possible values for the status of an interface are:

-  **Active**
-  **Down**
-  **Unknown**
-  **Warning**

# ITP Status Definitions

ITP status definitions include this information:

- [Status Definitions for Application Servers, page E-4](#)
- [Status Definitions for Application Server Processes, page E-4](#)
- [Status Definitions for Application Server Process Associations, page E-4](#)
- [Status Definitions for ITP Interfaces, page E-5](#)
- [Status Definitions for Links, page E-6](#)
- [Status Definitions for Linksets, page E-7](#)
- [Status Definitions for Signaling Gateway Mated Pairs, page E-7](#)
- [Status Definitions for Signaling Points, page E-7](#)

## Status Definitions for Application Servers

Possible values for the current status of the application server are:

-  **Active**—The application server is available and application traffic is active. At least one application server process serving this application server is Active.
-  **Down**—The application server is not available. All application server processes that serve this application server are Down. This is the initial status for application servers.
-  **Inactive**—The application server is available, but no application traffic is active (that is, at least one application server process is Inactive, and no application server process is Active).
-  **Pending**—The last remaining Active application server process serving this application server has become Inactive or Down. The next status for this application server will be Active, Inactive, or Down, depending on the recovery timer, and whether an application server process can become Active.
-  **Shutdown**—An administrator has forced the application server to an unavailable state.
-  **Unknown**—The MWTM cannot determine the current status of the application server.
-  **Warning**—The application server is Active, but one of these conditions exists:
  - At least one application server process association for this application server is not fully functional.
  - A signaling gateway-mated pair has been defined for this signaling point, but no application server exists on the mate.
  - The mate's application server is not Active.

## Status Definitions for Application Server Processes

Possible values for the current status of the application server process are:

-  **Unknown**—The MWTM cannot determine the current status of the application server process.
-  **Unmanaged**—The MWTM cannot determine the status of the application server process because there is no known SNMP stack on the node that hosts this application server process for the MWTM to query.

## Status Definitions for Application Server Process Associations

Possible values for the current status of the application server process association are:

-  **Active**—The remote peer at the application server process association is available and application traffic is active.
-  **Blocked**—The application server process association cannot receive normal data traffic, but it can send and receive control messages.
-  **Down**—The remote peer at the application server process association is not available, or the related SCTP association is down. This is the initial status for application server process associations.
-  **Inactive**—The remote peer at the application server process association is available, and the related SCTP association is up, but application traffic has stopped. The application server process association should not receive any data or SNMP messages for the application server.



-  **Pending**—The last remaining Active application server process serving this application server process association has become Inactive or Down. The next status for this application server process association will be Active, Inactive, or Down, depending on the recovery timer, and whether an application server process can become Active.
-  **Shutdown**—An administrator has forced the application server process association to an unavailable state.
-  **Unknown**—The MWTM cannot determine the current status of the application server process association.
-  **Warning**—The application server process association is Active, but some underlying facility is not fully functional.

## Status Definitions for ITP Interfaces

This section provides definitions for these statuses:

- [Admin Status, page E-8](#)
- [Operational Status, page E-8](#)
- [Status, page E-10](#)

### Admin Status

Possible values for the administrative status of the interface are:

-  **Unknown**—Unknown administrative status
-  **Up**—Administratively up
-  **Shutdown**—Administratively down
-  **Testing**—Administrator is testing the interface

### Operational Status

Possible values for the operational status of the interface are:

-  **Unknown**—Unknown operational status.
-  **Up**—Interface is up.
-  **Down**—Interface is down.
-  **Testing**—Interface is in test mode.
-  **Dormant**—Interface is dormant.
-  **Not Present**—An interface component is missing.
-  **Lower Layer Down**—An interface is down because of a lower-layer interface.

## Status

Possible values for the status of an interface are:

-  **Active**
-  **Down**
-  **Unknown**
-  **Warning**

## Status Definitions for Links

Possible values for the current status of the link are:

-  **Active**—The link is currently fully functional.
-  **Blocked**—Traffic on this link is disabled by protocol.
-  **Failed**—An error is preventing traffic from flowing on this link, or the associated linkset has been set to Shutdown status.

A link can be Failed from an MTP3 perspective, but control messages might still be sent or received on the link, resulting in changing packet/second and bit/second rates. The rates might also be different at each end of the link, depending on the reason for the failure and the timing related to each endpoint.

-  **InhibitLoc**—A local ITP administrator has set the link to prevent traffic from flowing.
-  **InhibitRem**—A remote ITP administrator has set the link to prevent traffic from flowing.
-  **Shutdown**—An ITP administrator has set the link to prevent traffic from flowing.
-  **Unknown**—Either the node associated with this link has failed to respond to an SNMP request, or the MWTM found that the link no longer exists.

When you physically delete a link, the Status field shows Unknown until you delete the link from the MWTM database.

-  **Warning**—The link is active and traffic is flowing, but one or more of these situations has occurred:
  - The link is congested.
  - The link has exceeded the defined Receive Utilization % or Send Utilization %.
  - One or more of the local or remote IP addresses defined for SCTP is not active.

## Status Definitions for Linksets

Possible values for the current status of the linkset are:

-  **Active**—The linkset is currently fully functional.
-  **Shutdown**—An ITP administrator has set the linkset to prevent traffic from flowing. When a linkset is set to Shutdown, all its associated links are set to Failed by Cisco IOS.
-  **Unavailable**—An error is preventing traffic from flowing on this linkset.
-  **Unknown**—Either the node associated with this linkset has failed to respond to an SNMP request, or the MWTM found that the linkset no longer exists.
-  **Warning**—The linkset is active, but one or more links in the linkset is congested or is in Failed, Unknown, or Warning status, and is not Ignored. At least one link is available and can carry traffic.

## Status Definitions for Signaling Gateway Mated Pairs

Possible values for the current status of the signaling gateway-mated pair are:

-  **Active**—The signaling gateway-mated pair is available and application traffic is active.
-  **Down**—The signaling gateway-mated pair is not available.
-  **Inactive**—The signaling gateway-mated pair is available, but application traffic has stopped.
-  **Shutdown**—An administrator has forced the signaling gateway-mated pair to an unavailable state.
-  **Unknown**—The MWTM cannot determine the current status of the signaling gateway-mated pair.
-  **Warning**—The signaling gateway-mated pair is Active, but some underlying facility is not fully functional.

## Status Definitions for Signaling Points

Possible values for the current status of the signaling point are:

-  **Active**—The signaling point is currently fully functional.
-  **Unknown**—The MWTM cannot poll the node associated with the signaling point.
-  **Unmanaged**—The MWTM cannot discover the signaling point. It is not an ITP node.
-  **Warning**—The signaling point is active, but one or more associated links or linksets is in Failed, Unavailable, Unknown, or Warning status and is not flagged as Ignored.

## RAN-O Status Definitions

RAN-O status definitions include this information:

- [Status Definitions for RAN-O Interfaces, page E-8](#)
- [Status Definitions for Cards, page E-10](#)
- [Status Definitions for RAN-O Backhauls, page E-10](#)

## Status Definitions for RAN-O Interfaces

This section provides definitions for these statuses:

- [Admin Status, page E-8](#)
- [Operational Status, page E-8](#)
- [Connect State for GSM Abis, page E-8](#)
- [Connect State for UMTS Iub, page E-9](#)
- [Alarm States, page E-9](#)
- [Redundancy State, page E-10](#)
- [Status, page E-10](#)

### Admin Status

Possible values for the administrative status of the interface are:

-  **Unknown**—Unknown administrative status
-  **Up**—Administratively up
-  **Shutdown**—Administratively down
-  **Testing**—Administrator is testing the interface

### Operational Status

Possible values for the operational status of the interface are:

-  **Unknown**—Unknown operational status.
-  **Up**—Interface is up.
-  **Down**—Interface is down.
-  **Testing**—Interface is in test mode.
-  **Dormant**—Interface is dormant.
-  **Not Present**—An interface component is missing.
-  **Lower Layer Down**—An interface is down because of a lower-layer interface.

### Connect State for GSM Abis

Possible values for the connect state of a Global System for Mobile Communications (GSM) interface are:

-  **Connected**—The node is monitoring local and remote alarm status.
-  **Disconnected**—The system ignores the local alarm status. The local transmitter on the short-haul is disabled. Capability messages are transmitted to the remote describing the provisioning. The system stays disconnected until the remote capabilities are known and the peer state transitions to connected.
-  **Send Connect**—One or more attempts have been made to connect to remote peer.
-  **Receive Connect**—The local peer has received a connect request from the remote peer.
-  **Connect Rejected**—Connection was rejected.

 **ACK Connect**—The initial connect request was sent and acknowledged by remote peer. The local peer is now waiting for a connect request from the remote peer.

 **Check Connect**—The local peer has reason to believe its remote peer has failed. Additional tests are being processed to verify peer's state.

## Connect State for UMTS Iub

Possible values for the connect state of a Universal Mobile Telecommunications System (UMTS) interface are:

 **Initialized**—The connection is starting initialization.

 **Starting**—The shorthaul interface is administratively active, but the backhaul interface is down.

 **Closed**—The backhaul interface is active, but the shorthaul is administratively closed.

 **Stopped**—Unable to connect to peer in specified time interval. Additional attempts will be tried based on peer request or restart timers.

 **Closing**—Connection closed by administration request.

 **Stopping**—Connection shut down by peer's Term-Request. Will transition to stopped state.

 **Connect Sent**—Connection request sent to peer.

 **ACK Received**—Connection request sent and acknowledgement has been received from peer. Now waiting for peer's connection request.

 **ACK Sent**—Connection request received and acknowledgement has been sent to peer. Connection request sent and waiting for peer's acknowledgement.

 **Open**—Connection open and available for traffic.

## Alarm States

The alarm states for a UMTS Iub interface include:

- Local Receive Alarm State
- Local Transmit Alarm State
- Remote Receive Alarm State
- Remote Transmit Alarm State

Possible values for these alarm states are:

 **Remote Alarm**—Indicates a problem at the remote end. The alarm generated by the remote interface in the E1/T1 data stream is sent and no other action is required.

 **No Alarm**—No alarm is present.

 **Local Alarm**—Indicates local interface problem. The interface has not received synchronization from the GSM node. The node stops transmitting backhaul samples.

 **Received Alarm**—Indicates receive problem in the local node. The remote node stops transmitting backhaul data and indicates a blue alarm.

 **Alarm State Unavailable**—Indicates the alarm state is not available. This state only applies to the remote and occurs when the peer connection is inactive.

## Redundancy State

Possible values for the redundancy state of GSM Abis or UMTS Iub interfaces are:

-  **Active**—Active owner of interface.
-  **Standby**—Active owner of interface.

## Status

Possible values for the status of an interface are:

-  **Active**—The interface is currently fully functional.
-  **Down**—The interface is not available.
-  **Unknown**—The MWTM cannot determine the current status of the interface.
-  **Warning**—The interface is Active, but some underlying object is not fully functional.

## Status Definitions for Cards

Possible values for cards in Cisco Optical Networking System (ONS) nodes are:

-  **Active**—The card is currently fully functional.
-  **Not Present**—Preconfigured but not inserted in the ONS chassis
-  **Failed**—Not functional
-  **Warning**—Not in configured protection state
-  **Unknown**—Failed SNMP

## Status Definitions for RAN-O Backhauls

Possible values for RAN backhauls are:

-  **Active**—The RAN backhaul is currently fully functional.
-  **Unknown**—The MWTM cannot determine the current status of the RAN backhaul.
-  **Warning**—At least one of the shorthaul interfaces or IP backhaul interfaces is not active
-  **Failed**—None of the shorthaul or IP backhaul interfaces are active

## mSEF Status Definitions

mSEF status definitions include the following:

- [Status Definitions for APNs, page E-10](#)

## Status Definitions for APNs

Possible values for the current APN status include:

-  **Active**—The APN is currently fully functional.

 **Warning**—An APN Instance associated with a top-level APN is not active.

 **Unknown**—The node failed to respond to an SNMP request.







# APPENDIX **F**

## MIB Reference

---

This appendix contains:

- [BWG Specific MIBs, page F-1](#)
- [Common MIBs, page F-2](#)
- [CSG1 Specific MIBs, page F-5](#)
- [CSG2 Specific MIBs, page F-6](#)
- [GGSN Specific MIBs, page F-6](#)
- [HA Specific MIBs, page F-7](#)
- [ITP Specific MIBs, page F-8](#)
- [IPRAN Specific MIBs, page F-10](#)

## BWG Specific MIBs

The Cisco Mobile Wireless Transport Manager (MWTM) queries this BWG specific Management Information Base (MIB):

| MIB                      | Description                                       |
|--------------------------|---------------------------------------------------|
| CISCO-ASN-GATEWAY-MIB.my | Manages Cisco's Broadband Wireless Gateway (BWG). |

| MIB                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-SLB-EXT-MIB.my | Supports Server Load Balancing Manager(s). This MIB extends the SLB management functionality in the CISCO-SLB-MIB. The Cisco Content Switching Module (CSM) product is the first SLB product to support this MIB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| CISCO-SLB-MIB.my     | <p>Supports Server Load Balancing Manager(s), such as the Cisco IOS SLB product.</p> <p>This MIB includes instrumentation for the manager-side implementation of the Dynamic Feedback Protocol (DFP). A DFP uses the DFP protocol to communicate with DFP agents in order to obtain information about Servers.</p> <p>This MIB includes the objects required for implementing the load balancer management side of the Server/Application State Protocol (SASP). The load balancer is responsible for registering Members with a SASP-Agent. A Member is an entity that is defined on the load balancer to service Internet traffic. The responsibility of the Agent is to monitor the Members, and report a recommended weight to the load balancer. The weight is then used in load balancing decisions.</p> |

## Common MIBs

The MWTM queries these general MIBs, listed in alphabetical order:

| MIB                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ATM-MIB.my                 | Module for ATM and AAL5-related objects for managing ATM interfaces, ATM virtual links, ATM cross-connects, AAL5 entities, and AAL5 connections.                                                                                                                                                                                                                                                                                                |
| ATM-TC-MIB.my              | Provides Textual Conventions and OBJECT-IDENTITY Objects to be used by ATM systems.                                                                                                                                                                                                                                                                                                                                                             |
| CISCO-AAA-SERVER-MIB.my    | Provides configuration and statistics reflecting the state of authentication, authorization, and accounting (AAA) server operation in the node and AAA communications with external servers.                                                                                                                                                                                                                                                    |
| CISCO-ACCESS-ENVMON-MIB.my | Describes the additional status of the Environmental Monitor on those Cisco Access devices which support one.                                                                                                                                                                                                                                                                                                                                   |
| CISCO-CONFIG-MAN-MIB.my    | <p>Provides configuration management, primarily by tracking changes and saving the running configuration. This MIB represents a model of configuration data that exists in various locations:</p> <ul style="list-style-type: none"> <li>• running—In use by the running system</li> <li>• terminal—Logical or attached hardware</li> <li>• local—Saved locally in NVRAM or flash</li> <li>• remote—Saved to a server on the network</li> </ul> |

| MIB                                    | Description                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-ENHANCED-MEMPOOL-MIB.my          | Monitors the memory pools of all physical entities on a managed system.                                                                                                                                                                                                                                                                                             |
| CISCO-ENTITY-FRU-CONTROL-CAPABILITY.my | Provides additional capabilities for various platforms that are needed by the <i>CISCO-ENTITY-FRU-CONTROL-MIB</i> .                                                                                                                                                                                                                                                 |
| CISCO-ENTITY-FRU-CONTROL-MIB.my        | Monitors and configures the operational status of Field Replaceable Units (FRUs) of the system listed in the Entity-MIB (RFC 2037) entPhysicalTable. FRUs include assemblies such as power supplies, fans, processor modules, interface modules, and so forth.                                                                                                      |
| CISCO-ENVMON-MIB.my                    | Provides environmental monitoring information on Cisco ITPs.                                                                                                                                                                                                                                                                                                        |
| CISCO-EPM-NOTIFICATION-MIB.my          | Defines the trap structure that carries the identity and status information of the managed object. The MWTM can send internal events as traps defined in this MIB to third-party network management system (NMS) applications for further processing.                                                                                                               |
| CISCO-FLASH-MIB.my                     | Provides management of Cisco Flash Devices.                                                                                                                                                                                                                                                                                                                         |
| CISCO-HSRP-EXT-MIB.my                  | Provides an extension to the <i>CISCO-HSRP-MIB</i> which defines Cisco's proprietary Hot Standby Routing Protocol (HSRP). The extensions cover assigning of secondary HSRP IP addresses and modifying an HSRP group's priority by tracking the operational status of interfaces.                                                                                    |
| CISCO-HSRP-MIB.my                      | Provides a means to monitor and configure the Cisco IOS proprietary Hot Standby Router Protocol (HSRP). Cisco HSRP protocol is defined in RFC2281.                                                                                                                                                                                                                  |
| CISCO-ICSUDSU-MIB.my                   | Integrated CSU/DSU MIB module for T1 and switched 56 kbps interfaces.                                                                                                                                                                                                                                                                                               |
| CISCO-IF-EXTENSION-MIB.my              | Extension to the <i>CISCO-IETF-SCTP-MIB</i> used to provide additional information to manage the Stream Control Transmission Protocol (RFC 2960).                                                                                                                                                                                                                   |
| CISCO-MEMORY-POOL-MIB.my               | Module for monitoring memory pools.                                                                                                                                                                                                                                                                                                                                 |
| CISCO-PROCESS-MIB.my                   | Shows memory and CPU utilization on Cisco nodes. CPU utilization gives a general idea of how busy the processor is. The numbers are a ratio of the current idle time divided by the longest idle time.                                                                                                                                                              |
| CISCO-PRODUCTS-MIB.my                  | Defines the object identifiers that are assigned to various hardware platforms, and hence are returned as values for sysObjectID.                                                                                                                                                                                                                                   |
| CISCO-QOS-PIB-MIB.my                   | Cisco QoS Policy PIB for provisioning QoS policy.                                                                                                                                                                                                                                                                                                                   |
| CISCO-RF-MIB.my                        | Provides configuration control and status for the Redundancy Framework (RF) subsystem. RF provides a mechanism for logical redundancy of software functionality and is designed to support 1-to-1 redundancy on processor cards. Redundancy is concerned with the duplication of data elements and software functions to provide an alternative in case of failure. |

| MIB                         | Description                                                                                                                                                                                                                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-RTTMON-MIB.my         | Defines a MIB for Round Trip Time (RTT) monitoring of a list of targets, using a variety of protocols.                                                                                                                                                                                               |
| CISCO-SMI.my                | Defines the Structure of Management Information for the Cisco enterprise.                                                                                                                                                                                                                            |
| CISCO-STACK-MIB.my          | Provides configuration and runtime status for chassis, modules, ports, and so on, on the Catalyst systems.                                                                                                                                                                                           |
| CISCO-SYSLOG-MIB.my         | Provides a means of gathering syslog messages generated by the Cisco IOS. The MWTM can send internal events as traps defined in this MIB to third-party NMS applications for further processing.                                                                                                     |
| CISCO-TC.my                 | Defines textual conventions used throughout Cisco enterprise MIBs.                                                                                                                                                                                                                                   |
| CISCO-VTP-MIB.my            | Module for entities implementing the VTP protocol and VLAN management.                                                                                                                                                                                                                               |
| ENTITY-MIB.my               | Module that represents multiple logical entities supported by a single SNMP agent. This MIB is based on RFC 2737. For more information on entity MIBs, see RFC 2037 section 3.                                                                                                                       |
| FDDI-SMT73-MIB.my           | Contains information for FDDI (Fiber Distributed Data Interface).                                                                                                                                                                                                                                    |
| HCNUM-TC.my                 | Contains textual conventions for high capacity data types. This module addresses an immediate need for data types not directly supported in the SMIv2. This short-term solution is meant to be deprecated when a long-term solution is deployed.                                                     |
| IANAifType-MIB.my           | Defines the IANAifType Textual Convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable.                                                                                                                                                                          |
| IF-MIB.my                   | Describes generic objects for network interface sublayers. This MIB is an updated version of MIB-II's ifTable, and incorporates the extensions defined in RFC 1229.                                                                                                                                  |
| IMA-MIB.my                  | Module that manages ATM Forum Inverse Multiplexing for ATM (IMA) interfaces.                                                                                                                                                                                                                         |
| INET-ADDRESS-MIB.my         | Defines textual conventions for representing Internet addresses. An Internet address can be an IPv4 address, an IPv6 address, or a DNS domain name. This module also defines textual conventions for Internet port numbers, autonomous system numbers, and the length of an Internet address prefix. |
| OLD-CISCO-INTERFACES-MIB.my | Defines interfaces for the Cisco enterprise.                                                                                                                                                                                                                                                         |
| OLD-CISCO-SYS-MIB.my        | Provides a means of gathering basic information for an IOS node.                                                                                                                                                                                                                                     |
| PerfHist-TC-MIB.my          | Provides Textual Conventions to be used by systems supporting 15 minute-based performance history counts.                                                                                                                                                                                            |
| RFC1213-MIB.my              | Provides basic management information on the ITP (RFC 1213).                                                                                                                                                                                                                                         |
| RFC-1406-MIB.my             | Contains DS1 (T1/E1) line information.                                                                                                                                                                                                                                                               |

| MIB                    | Description                                                                                                                                                                                                    |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RMON-MIB.my            | Remote network monitoring devices, often called monitors or probes, are instruments that exist for the purpose of managing a network. This MIB defines objects for managing remote network monitoring devices. |
| RMON2-MIB.my           | Module for managing remote monitoring device implementations. This MIB module augments the original <i>RMON MIB</i> as specified in RFC 1757.                                                                  |
| SNMP-FRAMEWORK-MIB.my  | Defines the SNMP Management Architecture.                                                                                                                                                                      |
| SNMP-TARGET-MIB.my     | Defines the MIB objects that provide mechanisms to remotely configure the parameters used by an SNMP entity for the generation of SNMP messages.                                                               |
| SNMPv2-CONF.my         | Defines SNMPv2 conformance.                                                                                                                                                                                    |
| SNMPv2-MIB.my          | Defines SNMPv2 entities.                                                                                                                                                                                       |
| SNMPv2-SMI.my          | Defines the Structure of Management Information for SNMPv2.                                                                                                                                                    |
| SNMPv2-TC.my           | Defines textual conventions for SNMPv2.                                                                                                                                                                        |
| TOKEN-RING-RMON-MIB.my | Contains Token Ring monitoring information.                                                                                                                                                                    |

## CSG1 Specific MIBs

The MWTM queries this CSG1 specific MIB:

| MIB                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-CSG-MIB.my     | Supports the Cisco Content Services Gateway (CSG) product. It includes five traps and four tables that enable querying CSG resource statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| CISCO-SLB-EXT-MIB.my | Supports Server Load Balancing Manager(s). This MIB extends the SLB management functionality in the CISCO-SLB-MIB. The Cisco Content Switching Module (CSM) product is the first SLB product to support this MIB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| CISCO-SLB-MIB.my     | <p>Supports Server Load Balancing Manager(s), such as the Cisco IOS SLB product.</p> <p>This MIB includes instrumentation for the manager-side implementation of the Dynamic Feedback Protocol (DFP). A DFP uses the DFP protocol to communicate with DFP agents in order to obtain information about Servers.</p> <p>This MIB includes the objects required for implementing the load balancer management side of the Server/Application State Protocol (SASP). The load balancer is responsible for registering Members with a SASP-Agent. A Member is an entity that is defined on the load balancer to service Internet traffic. The responsibility of the Agent is to monitor the Members, and report a recommended weight to the load balancer. The weight is then used in load balancing decisions.</p> |

## CSG2 Specific MIBs

The MWTM queries this CSG2 specific MIB:

| MIB                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-CONTENT-SERVICES-MIB.my | Content Service is a capability to examine IP/TCP/UDP headers, payload and enable billing based on the content being provided.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CISCO-SLB-EXT-MIB.my          | Supports Server Load Balancing Manager(s). This MIB extends the SLB management functionality in the CISCO-SLB-MIB. The Cisco Content Switching Module (CSM) product is the first SLB product to support this MIB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CISCO-SLB-MIB.my              | Supports Server Load Balancing Manager(s), such as the Cisco IOS SLB product.<br><br>This MIB includes instrumentation for the manager-side implementation of the Dynamic Feedback Protocol (DFP). A DFP uses the DFP protocol to communicate with DFP agents in order to obtain information about Servers.<br><br>This MIB includes the objects required for implementing the load balancer management side of the Server/Application State Protocol (SASP). The load balancer is responsible for registering Members with a SASP-Agent. A Member is an entity that is defined on the load balancer to service Internet traffic. The responsibility of the Agent is to monitor the Members, and report a recommended weight to the load balancer. The weight is then used in load balancing decisions. |

## GGSN Specific MIBs

The MWTM queries these GGSN specific MIBs, listed in alphabetical order:

| MIB                             | Description                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-GGSN-EXT-MIB.my           | Extends extends the CISCO-GGSN-MIB and manages the Gateway GPRS Support Node (GGSN) devices.<br><br>A GGSN device provides interworking with external packet-data network of a particular GPRS service provider. It provides a combination of IP routing and GPRS specific functionality to support mobile users. |
| CISCO-GGSN-MIB.my               | Manages the Gateway GPRS Support Node (GGSN) devices.                                                                                                                                                                                                                                                             |
| CISCO-GGSN-QOS-MIB.my           | Manages the Quality of Service parameters of GGSN in a GPRS system.                                                                                                                                                                                                                                               |
| CISCO-GGSN-SERVICE-AWARE-MIB.my | Manages the service-aware feature of Gateway GPRS Support Node (GGSN). This MIB is an enhancement of the <i>CISCO-GGSN-MIB</i> .                                                                                                                                                                                  |

| MIB                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-GPRS-ACC-PT-MIB.my   | Supports access point configuration for GGSN in a GPRS system. GPRS [1] is a GSM network providing mobile wireless data communication services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| CISCO-GPRS-CHARGING-MIB.my | Manages the charging related function on the GGSN node of a GPRS system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CISCO-GTP-MIB.my           | Manages the GPRS Tunnelling Protocol (GTP) on GGSN and SGSN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| CISCO-IP-LOCAL-POOL-MIB.my | Defines the configuration and monitoring capabilities relating to local IP pools.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| CISCO-PSD-CLIENT-MIB.my    | Manages the client side functionality of the Persistent Storage Device (PSD).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| CISCO-SLB-EXT-MIB.my       | Supports Server Load Balancing Manager(s). This MIB extends the SLB management functionality in the CISCO-SLB-MIB. The Cisco Content Switching Module (CSM) product is the first SLB product to support this MIB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| CISCO-SLB-MIB.my           | <p>Supports Server Load Balancing Manager(s), such as the Cisco IOS SLB product.</p> <p>This MIB includes instrumentation for the manager-side implementation of the Dynamic Feedback Protocol (DFP). A DFP uses the DFP protocol to communicate with DFP agents in order to obtain information about Servers.</p> <p>This MIB includes the objects required for implementing the load balancer management side of the Server/Application State Protocol (SASP). The load balancer is responsible for registering Members with a SASP-Agent. A Member is an entity that is defined on the load balancer to service Internet traffic. The responsibility of the Agent is to monitor the Members, and report a recommended weight to the load balancer. The weight is then used in load balancing decisions.</p> |

## HA Specific MIBs

The MWTM queries these HA specific MIBs, listed in alphabetical order:

| MIB                        | Description                                                                                                                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-IP-LOCAL-POOL-MIB.my | Defines the configuration and monitoring capabilities relating to local IP pools.                                                                                                                                 |
| CISCO-MOBILE-IP-MIB.my     | Extension to the <i>IETF MIB</i> module defined in RFC-2006 for managing Mobile IP implementations.                                                                                                               |
| CISCO-SLB-EXT-MIB.my       | Supports Server Load Balancing Manager(s). This MIB extends the SLB management functionality in the CISCO-SLB-MIB. The Cisco Content Switching Module (CSM) product is the first SLB product to support this MIB. |

| MIB              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-SLB-MIB.my | <p>Supports Server Load Balancing Manager(s), such as the Cisco IOS SLB product.</p> <p>This MIB includes instrumentation for the manager-side implementation of the Dynamic Feedback Protocol (DFP). A DFP uses the DFP protocol to communicate with DFP agents in order to obtain information about Servers.</p> <p>This MIB includes the objects required for implementing the load balancer management side of the Server/Application State Protocol (SASP). The load balancer is responsible for registering Members with a SASP-Agent. A Member is an entity that is defined on the load balancer to service Internet traffic. The responsibility of the Agent is to monitor the Members, and report a recommended weight to the load balancer. The weight is then used in load balancing decisions.</p> |
| RFC2006-MIB.my   | Module for the Mobile IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## ITP Specific MIBs

The MWTM queries these ITP specific MIBs, listed in alphabetical order:

| MIB                        | Description                                                                                                                                                                                                                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-BITS-CLOCK-MIB.my    | Provides information on Building Integrated Timing Supply (BITS) clocking sources and operation modes. The MWTM can generate notifications to indicate when clocking sources change roles or become unavailable.                                                                                                         |
| CISCO-IETF-SCTP-EXT-MIB.my | Extension to <i>CISCO-IETF-SCTP-MIB</i> that provides additional information to manage SCTP (RFC 2960).                                                                                                                                                                                                                  |
| CISCO-IETF-SCTP-MIB.my     | The MIB module for managing SCTP protocol (RFC 2960).                                                                                                                                                                                                                                                                    |
| CISCO-ITP-ACL-MIB.my       | Manages access lists that control messages sent over SS7 networks using ITP.                                                                                                                                                                                                                                             |
| CISCO-ITP-ACT-MIB.my       | Provides information specified in ITU Q752 Monitoring and Measurements for SS7 networks. This information is used to manage messages sent over SS7 networks using ITP. This MIB has been deprecated and replaced by the <i>CISCO-ITP-GACT-MIB</i> .                                                                      |
| CISCO-ITP-DSMR-MIB.my      | Provides information about Distributed Short Message Routing for Short Message Service Center. This MIB will provide information used to control and measure SS7 messages signalling units in a SS7 Network. Message Signalling Units are routed based on information found in the SCCP, TCAP, MAP, and MAP-user layers. |
| CISCO-ITP-DSMR-SMPP-MIB.my | Provides information about Distributed Short Message Routing delivery using Short Message Peer-to-Peer protocol.                                                                                                                                                                                                         |
| CISCO-ITP-DSMR-UCP-MIB.my  | Provides information about Distributed Short Message Routing delivery using Universal Computer Protocol.                                                                                                                                                                                                                 |



| MIB                        | Description                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-ITP-GACT-MIB.my      | Provides information specified in ITU Q752 Monitoring and Measurements for SS7 networks. This information is used to manage messages sent over SS7 networks using ITP. This MIB replaces the <i>CISCO-ITP-ACT-MIB</i> and supports multiple instances of a signaling point in the same configuration.                                           |
| CISCO-ITP-GRT-MIB.my       | Manages information required to route messages sent over SS7 networks using ITP. This MIB replaces the <i>CISCO-ITP-RT-MIB</i> and supports multiple instances of a signaling point in the same configuration.                                                                                                                                  |
| CISCO-ITP-GSCCP-MIB.my     | Provides information specified in ITU Q752 Monitoring and Measurements for SS7 networks. This information is used to manage Signaling Connection Control Part (SCCP) messages sent over SS7 networks using ITP. This MIB replaces the <i>CISCO-ITP-SCCP-MIB</i> and supports multiple instances of a signaling point in the same configuration. |
| CISCO-ITP-GSP-MIB.my       | Manages signaling points and associated messages sent over SS7 networks using ITP. This MIB replaces the <i>CISCO-ITP-SP-MIB</i> and supports multiple instances of a signaling point in the same configuration.                                                                                                                                |
| CISCO-ITP-GSP2-MIB.my      | Provides information specified in ITU Q752 Monitoring and Measurements for SS7 networks. This information is used to manage messages sent over SS7 networks using ITP. This MIB replaces the <i>CISCO-ITP-SP2-MIB</i> and supports multiple instances of a signaling point in the same configuration.                                           |
| CISCO-ITP-MLR-MIB.my       | Provides information about Multi-Layer Routing (MLR). This information is used to control and measure SS7 message signaling units (MSUs) in an SS7 network.                                                                                                                                                                                     |
| CISCO-ITP-MONITOR-MIB.my   | Provides information about monitoring SS7 links. This information is used to manage the state of software used to collect all packets transported and received over an SS7 link.                                                                                                                                                                |
| CISCO-ITP-MSU-RATES-MIB.my | Provides information used to manage the number of MTP3 MSUs transmitted and received per processor. Many of the higher level protocols require several MSUs per transaction. Traffic capacity planning is based on MSUs, not transactions. This MIB provides information to determine current traffic.                                          |
| CISCO-ITP-RT-MIB.my        | Manages the route tables used to control messages sent over SS7 networks using ITP. This MIB has been deprecated and replaced by the <i>CISCO-ITP-GRT-MIB</i> .                                                                                                                                                                                 |
| CISCO-ITP-SCCP-MIB.my      | Manages SCCP messages sent over SS7 networks using ITP, and provides information specified in ITU Q752 Monitoring and Measurements for SS7 networks. This MIB has been deprecated and replaced by the <i>CISCO-ITP-GSCCP-MIB</i> .                                                                                                              |
| CISCO-ITP-SP-MIB.my        | Manages signaling points and associated linksets and links in SS7 networks using ITP.                                                                                                                                                                                                                                                           |

| MIB                     | Description                                                                                                                                                                                                                                                                                                                                |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-ITP-SP2-MIB.my    | Provides Quality of Service (QoS) information related to the configuration of an SS7 network. Also provides MTP3 event history information. This MIB has been deprecated and replaced by the <i>CISCO-ITP-GSP2-MIB</i> .                                                                                                                   |
| CISCO-ITP-TC-MIB.my     | Defines textual conventions used to manage nodes related to the SS7 network. The ITU documents that describe this technology are the ITU Q series, including: <ul style="list-style-type: none"> <li>ITU Q.700: Introduction to CCITT SS7</li> <li>ITU Q.701: Functional description of the message transfer part (MTP) of SS7.</li> </ul> |
| CISCO-ITP-XUA-MIB.my    | Manages MTP3 User Adaptation (M3UA) and SCCP User Adaptation (SUA) for ITP.                                                                                                                                                                                                                                                                |
| NetNumber-MIB.my        | Common Object Definitions for the NetNumber enterprise MIBs.                                                                                                                                                                                                                                                                               |
| NetNumber-Server-MIB.my | Common Object Definitions for all NetNumber Application Server products.                                                                                                                                                                                                                                                                   |
| TITAN-MIB.my            | Module for the NetNumber TITAN.                                                                                                                                                                                                                                                                                                            |

## IPRAN Specific MIBs

The MWTM queries these IPRAN specific MIBs, listed in alphabetical order:

| MIB                            | Description                                                                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CERENT-454-MIB.mib             | Defines the alarms and events for the Cisco ONS 15454. The MWTM processes each ONS event by creating an MWTM event with a severity that maps to the severity of the ONS event.                           |
| CERENT-ENVMON-MIB.mib          | Provides environmental status information.                                                                                                                                                               |
| CERENT-FC-MIB.mib              | Defines the managed objects for performance monitoring of supported Fibre Channel interfaces.                                                                                                            |
| CERENT-GLOBAL-REGISTRY.mib     | Provides the global registrations for all other CERENT MIB modules.                                                                                                                                      |
| CERENT-MSDWDM-MIB.mib          | Defines the managed objects for physical layer related interface configurations and objects for the protocol specific error counters for dense wavelength division multiplexing (DWDM) optical switches. |
| CERENT-OPTICAL-MONITOR-MIB.mib | Defines objects to monitor optical characteristics and set corresponding thresholds on the optical interfaces in a network element.                                                                      |
| CERENT-TC.mib                  | Provides the global Textual Conventions for all other CERENT MIB modules.                                                                                                                                |
| CISCO-IETF-PW-MIB.my           | Contains managed object definitions for Pseudo Wire operation.                                                                                                                                           |

| MIB                          | Description                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-IETF-PW-TC-MIB.my      | Used to identify the VC (together with some other fields) in the signaling session. Zero if the VC is set-up manually.                                         |
| CISCO-IP-RAN-BACKHAUL-MIB.my | Provides information on the optimization of IP-RAN traffic between the cell site and the aggregation node site. It handles both GSM Abis and UMTS Iub traffic. |
| MPLS-VPN-MIB.my              | Contains managed object definitions for the Multiprotocol Label Switching (MPLS)/Border Gateway Protocol (BGP) Virtual Private Networks (VPNs).                |

You can obtain the latest versions of these MIBs from one of these locations:

- The zip file *mibs.zip*, located at the top of the MWTM DVD Image, contains these MIBs.
- You can download these MIBs from the Cisco website:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>





# APPENDIX **G**

## Trap Reference

---

This appendix contains:

- [General Traps, page G-1](#)
- [ITP Specific Traps, page G-7](#)
- [IPRAN Specific Traps, page G-11](#)
- [mSEF Specific Traps, page G-12](#)

## General Traps

The Cisco Mobile Wireless Transport Manager (MWTM) supports these general traps/notifications, which apply to:

- IP Transfer Point (ITP) networks
- IP Radio Access Network (IPRAN) networks
- Mobile Services Exchange Framework (mSEF) networks, which include:
  - Content Services Gateway (CSG)
  - Gateway GPRS Support Node (GGSN)
  - Home Agent (HA)
  - Broadband Wireless Gateway (BWG)



### Note

Some traps are platform/IOS specific.

| Trap Name             | Description                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| authenticationFailure | An authenticationFailure trap signifies that the IP address is accessing this node using the wrong community string.                                                     |
| casServerStateChange  | An AAA server state change notification is generated whenever an AAA server connection state changes value. An AAA server state can be either <i>up</i> or <i>dead</i> . |

| Trap Name                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ccmCLIRunningConfigChanged              | This notification indicates that the running configuration of the managed system has changed from the CLI. If the managed system supports a separate configuration mode (where the configuration commands are entered under a configuration session which affects the running configuration of the system), then this notification is sent when the configuration mode is exited. During this configuration session there can be one or more running configuration changes. |
| cefcFRUInserted                         | The cefcFRUInserted notification indicates that a FRU was inserted. The varbind for this notification indicates the entPhysicalIndex of the inserted FRU, and the entPhysicalIndex of the FRU container.                                                                                                                                                                                                                                                                    |
| cefcFRURemoved                          | The cefcFRURemoved notification indicates that a FRU was removed. The varbind for this notification indicates the entPhysicalIndex of the removed FRU, and the entPhysicalIndex of the FRU container.                                                                                                                                                                                                                                                                       |
| cefcModuleStatusChange                  | This notification is generated when the value of cefcModuleOperStatus changes. It can be utilized by an NMS to update the status of the module it is managing.                                                                                                                                                                                                                                                                                                              |
| cefcPowerStatusChange                   | The cefcFRUPowerStatusChange notification indicates that the power status of a FRU has changed. The varbind for this notification indicates the entPhysicalIndex of the FRU, and the new operational-status of the FRU.                                                                                                                                                                                                                                                     |
| cHsrpStateChange                        | A cHsrpStateChange notification is sent when a cHsrpGrpStandbyState transitions to either active or standby state, or leaves active or standby state. There will be only one notification issued when the state change is from standby to active and vice versa.                                                                                                                                                                                                            |
| ciscoConfigManEvent                     | Notification of a configuration management event as recorded in ccmHistoryEventTable.                                                                                                                                                                                                                                                                                                                                                                                       |
| ciscoEnvMonFanNotification              | A ciscoEnvMonFanNotification trap is generated if any one of the fans in the fan array (where extant) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.                                                                                                                                                              |
| ciscoEnvMonRedundantSupply Notification | A ciscoEnvMonRedundantSupplyNotification trap is generated if the redundant power supply (where extant) fails. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.                                                                                                                                                            |

| Trap Name                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoEnvMonShutdownNotification      | A ciscoEnvMonShutdownNotification trap is generated if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it can be encoded and sent in the shortest amount of time possible. Even so, management applications should not rely on receiving such a notification as it might not be sent before the shutdown completes. |
| ciscoEnvMonTemperatureNotification   | A ciscoEnvMonTemperatureNotification trap is generated if the temperature measured at a given testpoint is outside the normal range for the testpoint (that is, is at the warning, critical, or shutdown stage). Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.             |
| ciscoEnvMonVoltageNotification       | A ciscoEnvMonVoltageNotification trap is generated if the voltage measured at a given testpoint is outside the normal range for the testpoint (that is, is at the warning, critical, or shutdown stage). Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.                     |
| ciscoFlashCopyCompletionTrap         | A ciscoFlashCopyCompletionTrap is sent at the completion of a flash copy operation if such a trap was requested when the operation was initiated.                                                                                                                                                                                                                                                                              |
| ciscoFlashDeviceChangeTrap           | A ciscoFlashDeviceChangeTrap is sent whenever a removable Flash device is inserted or removed.                                                                                                                                                                                                                                                                                                                                 |
| ciscoFlashDeviceInsertedNotif        | A ciscoFlashDeviceInsertedNotif notification is sent whenever a removable Flash device is inserted.                                                                                                                                                                                                                                                                                                                            |
| ciscoFlashDeviceInsertedNotifRev1    | A ciscoFlashDeviceInsertedNotif notification is sent whenever a removable Flash device is inserted<br>ciscoFlashDeviceInsertedNotifRev1 deprecates ciscoFlashDeviceInsertedNotif since it uses ciscoFlashDeviceName as a varbind which is deprecated.                                                                                                                                                                          |
| ciscoFlashDeviceRemovedNotif         | A ciscoFlashDeviceRemovedNotif notification is sent whenever a removable Flash device is removed.                                                                                                                                                                                                                                                                                                                              |
| ciscoFlashDeviceRemovedNotifRev1     | A ciscoFlashDeviceRemovedNotif notification is sent whenever a removable Flash device is removed.<br>ciscoFlashDeviceRemovedNotifRev1 deprecates ciscoFlashDeviceRemovedNotif since it uses ciscoFlashDeviceName as a varbind, which is deprecated.                                                                                                                                                                            |
| ciscoFlashMiscOpCompletionTrap       | A ciscoFlashMiscOpCompletionTrap is sent at the completion of a miscellaneous flash operation (enumerated in ciscoFlashMiscOpCommand) if such a trap was requested when the operation was initiated.                                                                                                                                                                                                                           |
| ciscoFlashPartitioningCompletionTrap | A ciscoFlashPartitioningCompletionTrap is sent at the completion of a partitioning operation if such a trap was requested when the operation was initiated.                                                                                                                                                                                                                                                                    |

| Trap Name                   | Description                                                                                                                                                                                                                                                                               |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoRFProgressionNotif     | A ciscoRFProgressionNotif trap is sent by the active redundant unit whenever its RF state changes or the RF state of the peer unit changes.                                                                                                                                               |
| ciscoRFSwactNotif           | A ciscoRFSwactNotif trap is sent by the newly active redundant unit whenever a switch of activity (SWACT) occurs. In the case where a SWACT event might be indistinguishable from a reset event, a network management station should use this notification to differentiate the activity. |
| cisco_authenticationFailure | An authenticationFailure trap signifies that the IP address is accessing this node using the wrong community string.                                                                                                                                                                      |
| cisco_coldStart             | A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration might be altered.                                                                                                                                        |
| cisco_linkDown              | A linkDown trap signifies a failure in one of the communication links represented in the node's configuration has occurred.                                                                                                                                                               |
| cisco_linkUp                | A linkUp trap signifies that one of the communication links represented in a node's configuration has come up.                                                                                                                                                                            |
| cisco_warmStart             | A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.                                                                                                                                            |
| clogMessageGenerated        | When a syslog message is generated by the node a clogMessageGenerated notification is sent. The sending of these notifications can be enabled/disabled via the clogNotificationsEnabled object.                                                                                           |
| coldStart                   | A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration might be altered.                                                                                                                                        |
| cpmCPUFallingThreshold      | A cpmCPUFallingThreshold trap is generated when CPU utilization is below the falling threshold.                                                                                                                                                                                           |
| cpmCPURisingThreshold       | A cpmCPURisingThreshold trap is generated when CPU utilization is above the rising threshold.                                                                                                                                                                                             |



| Trap Name                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| entConfigChange                    | <p>An entConfigChange notification is generated when the value of entLastChangeTime changes. It can be utilized by an NMS to trigger logical/physical entity table maintenance polls.</p> <p>An agent should not generate more than one entConfigChange notification-event in a given time interval (five seconds is the suggested default). A notification-event is the transmission of a single trap or inform PDU to a list of notification destinations.</p> <p>If additional configuration changes occur in the throttling period, then notification-events for these changes should be suppressed by the agent until the current throttling period expires. At the end of a throttling period, one notification-event should be generated if any configuration changes occurred since the start of the throttling period. In such a case, another throttling period is started right away.</p> <p>An NMS should periodically check the value of entLastChangeTime to detect any missed entConfigChange notification-events (for example, because of throttling or transmission loss).</p> |
| fallingAlarm                       | The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| linkDown                           | A linkDown trap signifies a failure in one of the communication links represented in the node's configuration has occurred.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| linkUp                             | A linkUp trap signifies that one of the communication links represented in a node's configuration has come up.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| risingAlarm                        | The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| rttMonConnectionChangeNotification | <p>This notification is only valid when the RttMonRttType is <i>echo</i> or <i>pathEcho</i>. An rttMonConnectionChangeNotification indicates that a connection to a target (not to a hop along the path to a target) has either failed on establishment or been lost and when reestablished. This causes rttMonCtrlOperConnectionLostOccurred to change value. If history is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not <i>echo</i> or <i>pathEcho</i>, the rttMonHistoryCollectionAddress object will be null.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| rttMonLpdDiscoveryNotification     | <p>A rttMonLpdDiscoveryNotification indicates that the LSP Path Discovery to the target PE has failed, and it also indicates the clearing of such condition. This causes rttMonLpdGrpStatsLPDFailOccurred to change value. When the rttMonLpdGrpStatsLPDFailOccurred is <i>false</i>, the instance value for rttMonLpdGrpStatsLPDFailCause is not valid.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Trap Name                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rttMonLpdGrpStatusNotification | A rttMonLpdGrpStatusNotification indicates that the LPD Group status rttMonLpdGrpStatsGroupStatus has changed, indicating some connectivity change to the target PE. This causes rttMonLpdGrpStatsGroupStatus to change value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| rttMonNotification             | A rttMonNotification indicates the occurrence of a threshold violation, and it indicates the previous violation has subsided for a subsequent operation. When the RttMonRttType is <i>pathEcho</i> , this notification will only be sent when the threshold violation occurs during an operation to the target and not to a hop along the path to the target. This also applies to the subsiding of a threshold condition. If history is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not <i>echo</i> or <i>pathEcho</i> , the rttMonHistoryCollectionAddress object will be null. rttMonReactVar defines the type of reaction that is configured for the probe (for example, jitterAvg). Trap definitions for the probes are in the rttMonReactTable, and each probe can have more than one trap definition for various types (for example, jitterAvg). So the object rttMonReactVar indicates the type (for example, packetLossSD) for which threshold violation traps have been generated. The object rttMonEchoAdminLSPSelector will be valid only for the probes based on <i>mplsLspPingAppl</i> RttMonProtocol. For all other probes it will be null. |
| rttMonThresholdNotification    | A rttMonThresholdNotification indicates the occurrence of a threshold violation for a RTT operation, and it indicates the previous violation has subsided for a subsequent RTT operation. This causes rttMonCtrlOperOverThresholdOccurred to change value. When the RttMonRttType is <i>pathEcho</i> , this notification will only be sent when the threshold violation occurs during an operation to the target and not to a hop along the path to the target. This also applies to the subsiding of a threshold condition. If history is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not <i>echo</i> or <i>pathEcho</i> the rttMonHistoryCollectionAddress object will be null.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| rttMonTimeoutNotification      | A rttMonTimeoutNotification indicates the occurrence of a timeout for a RTT operation, and it indicates the clearing of such a condition by a subsequent RTT operation. This causes rttMonCtrlOperTimeoutOccurred to change value. When the RttMonRttType is <i>pathEcho</i> , this notification will only be sent when the timeout occurs during an operation to the target and not to a hop along the path to the target. This also applies to the clearing of the timeout. If history is not being collected, the instance values for the rttMonHistoryCollectionAddress object will not be valid. When RttMonRttType is not <i>echo</i> or <i>pathEcho</i> , the rttMonHistoryCollectionAddress object will be null.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Trap Name                     | Description                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| rttMonVerifyErrorNotification | A rttMonVerifyErrorNotification indicates the occurrence of a data corruption in an RTT operation.                                             |
| warmStart                     | A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered. |

## ITP Specific Traps

The MWTM supports these ITP specific traps, listed in alphabetical order:

| Trap Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoBitsClockFreerun       | This trap is for Building Integrated Timing Supply (BITS) clocking sources. It is used to generate notifications to indicate when clocking source is unavailable. The internal clock will operate in freerun mode using appropriate local oscillator. Therefore, it does not provide synchronous clocking. This is the least stable of all operating modes.                                                                                                                                                                                                                                                                                                                                                                           |
| ciscoBitsClockHoldover      | This trap is for Building Integrated Timing Supply (BITS) clocking sources. It is used to generate notifications to indicate when clocking source is unavailable and the internal clock will operate in holdover mode. The network clock module has stored information about the incoming clock signal, it can faithfully reproduce the lost signal while in holdover mode until a switchover to another clock source occurs.                                                                                                                                                                                                                                                                                                         |
| ciscoBitsClockSource        | This trap is for Building Integrated Timing Supply (BITS) clocking sources. It is used to generate notifications to indicate when clocking sources change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ciscoGftDestStateChangeRev1 | <p>A ciscoGftDestStateChangeRev1 trap is generated whenever one or more destination changes states within the cgrtDestNotifWindowTimeRev1 duration. Latest state information at the end of cgrtDestNotifWindowTimeRev1 is provided.</p> <p>It may be necessary to suppress the sending of notification when a large number destinations change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for cgrtDestNotifWindowTimeRev1 and cgrtDestNotifMaxPerWindowRev1 objects. When the number of destination state changes exceed the specified value, the notification will provide a count of notifications that got suppressed for the remainder of the window.</p> |

| Trap Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoGrtDestStateChange     | <p>A ciscoGrtDestStateChange trap is generated whenever one or more destination changes states. This notification contains a list of destination state changes in the cgrtDestNotifChanges object. State changes are accumulated until the cgrtDestNotifChanges is full or the maximum delay time is reached. The delay time is specified by the cgrtDestNotifDelayTime object.</p> <p>It might be necessary to suppress the sending of notification when a large number destinations change state, due to the failure of some common resource. The number of notifications can be controlled by specifying values for cgrtDestNotifWindowTime and cgrtDestNotifMaxPerWindow objects. When the number of destination state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.</p> <p>This notification deprecates ciscoGrtDestStateChange.</p> |
| ciscoGrtMgmtStateChangeRev1 | <p>This notification is generated whenever one or more management routes change states within the cgrtMgmtNotifWindowTimeRev1 duration. Latest state information at the end of cgrtMgmtNotifWindowTimeRev1 is provided.</p> <p>It may be necessary to suppress the sending of notification when a large number of routes change state, due the failure of some common resource. The number of notifications can be controlled by specifying values for cgrtMgmtNotifWindowTimeRev1 and cgrtMgmtNotifMaxPerWindowRev1 objects. When the number of route state changes exceed the specified value, the last notification will provide a count of notifications that got suppressed for the remainder of the window.</p> <p>This notification deprecates ciscoGrtMgmtStateChange.</p>                                                                                                                                                    |
| ciscoGrtMgmtStateChange     | <p>A ciscoGrtMgmtStateChange trap is generated whenever one or more management routes change state. This notification contains a list of management route state changes in the cgrtMgmtNotifChanges object. State changes are accumulated until the cgrtMgmtNotifChanges is full or the maximum delay time is reached. The delay time is specified by the cgrtMgmtNotifDelayTime object.</p> <p>It might be necessary to suppress the sending of notification when a large number of routes change state, due to the failure of some common resource. The number of notifications can be controlled by specifying values for cgrtMgmtNotifWindowTime and cgrtMgmtNotifMaxPerWindow objects. When the number of route state changes exceed the specified value the last notification will indicate that notifications are suppressed for the remainder of the window.</p>                                                              |
| ciscoGrtRouteTableLoad      | <p>A ciscoGrtRouteTableLoad trap is generated whenever a load operation is started or completed. Route table configurations can be loaded by CLI requests. In addition, route tables can loaded using configuration statements. This allows route tables to be reloaded whenever a node restarts.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Trap Name                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoGsccpGttErrors         | This notification is generated whenever any global title error is encountered in last interval specified by the cgsccpGttErrorPeriod and the cgsccpInstErrorIndicator will be set to true. The notification will also be generated when errors have abated. The notification is generated after the number of recovery intervals as specified by the cgsccpGttErrorRecoveryCount object has passed without any global title errors.                                                                                                                                                                                                                                                                                           |
| ciscoGsccpGttLoadTable      | A ciscoGsccpGttLoadTable trap is generated whenever a load operation is started or completes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ciscoGsccpGttMapStateChange | A ciscoGsccpGttMapStateChange is generated when a mated application subsystem changes to a new state. The value of cgsccpGttMapSsStatus indicates the new state for the subsystem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ciscoGspCongestionChange    | A ciscoGspCongestionChange trap is generated when a link changes to a new congestion level as specified by the cgspLinkCongestionState object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ciscoGspIsolation           | This notification indicates the instance specified by cgspInstDisplayName and cgspInstDescription has become isolated. All linkset used to connect MTP3 node (instance) are unavailable. Isolation is ended when any linkset supported by this instance reaches the active state.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ciscoGspLinkRcvdUtilChange  | A ciscoGspLinkRcvdUtilChange trap is generated when the cgspLinkUtilStateRcvd changes states.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ciscoGspLinkSentUtilChange  | A ciscoGspLinkSentUtilChange trap is generated when the cgspLinkUtilStateSent changes states.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ciscoGspLinksetStateChange  | A ciscoGspLinksetStateChange trap is generated when a linkset changes to a new state. The value of cItpSpLinksetState indicates the new state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ciscoGspLinkStateChange     | A ciscoGspLinkStateChange trap is generated when a link changes to a new state. The value of cItpSpLinkState indicates the new state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ciscoItpMsuRateState        | <p>This notification is generated once for the interval specified by the cimrMsuRateNotifyInterval object when the cimrMsuTrafficRateState object has the following state transitions:</p> <ul style="list-style-type: none"> <li>• acceptable to warning</li> <li>• acceptable to overloaded</li> <li>• warning to overloaded</li> </ul> <p>At the end of the interval specified by the cimrMsuRateNotifyInterval object another notification will be generated if the current state is different from state sent in last notification even if the state transition is not one of the previously mentioned transitions. When the cimrMsuRateNotifyInterval is set to zero all state changes will generate notifications.</p> |

| Trap Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoItpXuaAsStateChange          | A ciscoItpXuaAsStateChange trap is generated when an AS changes to a new state. The value of cItpXuaAsState indicates the new state for the AS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ciscoItpXuaAspAssocStateChange    | The ciscoItpXuaAspAssocStateChange trap is generated when the association used to connect to the ASP changes state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ciscoItpXuaAspCongChange          | A ciscoItpXuaAspCongChange trap is generated when an ASP changes to a congestion level as specified by the cItpXuaAspCongLevel object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ciscoItpXuaAspDestAddrStateChange | The ciscoItpXuaAspDestAddrStateChange trap is generated when a destination IP address used by ASP changes state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ciscoItpXuaSgmDestAddrStateChange | The ciscoItpXuaSgmDestAddrStateChange trap is generated when a destination IP address used by SG Mate changes state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ciscoItpXuaAspStateChange         | A ciscoItpXuaAspStateChange trap is generated when an ASP changes to a new state. The value of cItpXuaAspAsState indicates the new state for the ASP that is serving the AS specified by cItpXuaAsDisplayName.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ciscoItpXuaSgmAssocStateChange    | The ciscoItpXuaSgmAssocStateChange trap is generated when the association used to connect to the SG Mate changes state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ciscoItpXuaSgmCongChange          | A ciscoItpXuaSgmCongChange trap is generated when an SGMP changes to a congestion level as specified by the cItpXuaSgmCongLevel object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| ciscoItpXuaSgmStateChange         | A ciscoItpXuaSgmStateChange trap is generated when an SG Mate changes to a new state. The value of cItpXuaSgmState indicates the new state for the SG Mate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ciscoMlrTableLoad                 | A ciscoMlrTableLoad trap is generated when a load operation is started or completed. Route table configurations can be loaded by CLI requests. In addition, route tables can be loaded using configuration statements, which allows route tables to be reloaded whenever a node restarts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| cItpRouteStateChange              | <p>A cItpRouteStateChange trap is generated whenever one or more route destination status changes states and includes the count of all route state changes. This notification contains a list of route state changes in the cItpRtNotifInfoStateChanges object. State changes are accumulated until the cItpRtNotifInfoStateChanges is full or the maximum delay time is reached. The delay time is specified by the cItpRtChangeNotifDelayTime object.</p> <p>It might be necessary to suppress the sending of notification when a large number of route change states, due to the failure of some common resource. The number of notifications can be controlled by specifying values for cItpRtChangeNotifWindowTime and cItpRtChangeNotifMaxPerWindow objects. When the number of route state changes exceeds the specified value, the last notification will indicate that notifications are suppressed for the remainder of the window.</p> |

| Trap Name                      | Description                                                                                                                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cItpSccpGttMapStateChange      | A cItpSccpGttMapStateChange trap is generated when a mated application subsystem changes to a new state. The value of cItpSccpGttMapSsStatus indicates the new state for the subsystem. |
| cItpSpCongestionChange         | A cItpSpCongestionChange trap is generated when a link changes to a new congestion level as specified by the cItpLinkCongestionState object.                                            |
| cItpSpLinkRcvdUtilChange       | A cItpSpLinkRcvdUtilChange trap is generated when the cItpSpLinkUtilStateRcvd changes states.                                                                                           |
| cItpSpLinkSentUtilChange       | A cItpSpLinkSentUtilChange trap is generated when the cItpSpLinkUtilStateSent changes states.                                                                                           |
| cItpSpLinksetStateChange       | A cItpSpLinksetStateChange trap is generated when a linkset changes to a new state. The value of cItpSpLinksetState indicates the new state.                                            |
| cItpSpLinkStateChange          | A cItpSpLinkStateChange trap is generated when a link changes to a new state. The value of cItpSpLinkState indicates the new state.                                                     |
| cSctpExtDestAddressStateChange | A cSctpExtDestAddressStateChange trap is generated when the state transition of cSctpAssocRemAddressStatus has occurred.                                                                |

## IPRAN Specific Traps

- [RAN-O Specific Traps, page G-11](#)
- [PWE3 Specific Traps, page G-12](#)

## RAN-O Specific Traps

The MWTM supports these RAN-O specific traps, listed in alphabetical order:

| Trap Name                   | Description                                                                                                                                                                                                             |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cerent454Events             | The CERENT-454-MIB defines the events and alarms that are raised by the ONS 15454. The MWTM processes each ONS event by creating an MWTM event with a severity that maps to the severity of the ONS event.              |
| ciscoIpRanBackHaulGsmAlarm  | A ciscoIpRanBackHaulGsmAlarm trap is generated when the values of these objects change: connect state, local alarm state, remote alarm state, and redundancy state.                                                     |
| ciscoIpRanBackHaulUmtsAlarm | A ciscoIpRanBackHaulUmtsAlarm trap is generated when the values of these objects change: connect state, received local state, received remote state, transmit local state, transmit remote state, and redundancy state. |

## PWE3 Specific Traps

The MWTM supports these PWE3 specific traps, listed in alphabetical order:

| Trap Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cpwVcDown | <p>The cpwVcDown trap is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the down(2) state from some other state. The included values of cpwVcOperStatus MUST all be set equal to this down(2) state. The two instances of cpwVcOperStatus in this notification indicate the range of indexes that are affected. Note that all the indexes of the two ends of the range can be derived from the instance identifiers of these two objects.</p> <p>For cases where a contiguous range of cross-connects have transitioned into the down(2) state at roughly the same time, the device SHOULD issue a single notification for each range of contiguous indexes in an effort to minimize the emission of a large number of notifications. If a notification has to be issued for just a single cross-connect entry, then the instance identifier (and values) of the two cpwVcOperStatus objects MUST be identical.</p>              |
| cpwVcUp   | <p>This notification is generated when the cpwVcOperStatus object for one or more contiguous entries in cpwVcTable are about to enter the up(1) state from some other state. The included values of cpwVcOperStatus MUST both be set equal to this new state (that is, up(1)).</p> <p>The two instances of cpwVcOperStatus in this notification indicate the range of indexes that are affected. Note that all the indexes of the two ends of the range can be derived from the instance identifiers of these two objects. For cases where a contiguous range of cross-connects have transitioned into the up(1) state at roughly the same time, the device SHOULD issue a single notification for each range of contiguous indexes in an effort to minimize the emission of a large number of notifications. If a notification has to be issued for just a single cross-connect entry, then the instance identifier (and values) of the two cpwVcOperStatus objects MUST be the identical.</p> |

## mSEF Specific Traps

The MWTM supports these mSEF specific traps, listed in alphabetical order:

- [Generic mSEF Traps, page G-13](#)
- [CSG1 Traps, page G-14](#)
- [CSG2 Traps, page G-15](#)
- [GGSN Traps, page G-16](#)



- [BWG Traps, page G-18](#)
- [HA Traps, page G-19](#)

## Generic mSEF Traps

| Trap Name                      | Description                                                                                                                            |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| ciscoSlbRealState Change       | The notification generated when a real server changes to a new state. The value of slbRealServerState indicates the new state.         |
| ciscoSlbSaspAgentState Change  | The notification generated when a SASP (Server to Application State Protocol) Agent changes to a new state.                            |
| ciscoSlbSaspState Change       | The notification generated when the SASP functionality has been enabled or disabled on the Load Balancer.                              |
| ciscoSlbVServerState Change    | The notification generated when a virtual server state is changed.                                                                     |
| ciscoSlbVServerVIP StateChange | The notification generated when configuration or association of virtual server IP address (VIP) changes.                               |
| ciscoSlbVirtualState Change    | The notification generated when a virtual server changes to a new state. The value of slbVirtualServerState indicates the new state.   |
| cslbxFtStateChange             | The notification generated when the Fault Tolerance process changes to a new state. The value of cslbxFtState indicates the new state. |

## CSG1 Traps

| Trap Name                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoCsgAgentLostRecordEvent    | <p>This notification is issued when <code>csgAgentNotifsEnabled</code> is set to true, and the CSG must discard accounting records that should be sent to the billing mediation agent.</p> <p>Initially, <code>csgAgentLostRecords</code> is set to 0. When a record is discarded, <code>csgAgentLostRecords</code> is incremented, a period timer is started, and this notification is issued. The NMS and the agent save this value. The agent continues to increment <code>csgAgentLostRecords</code> each time a record is lost. When the period timer expires, the agent compares the current value of <code>csgAgentLostRecords</code> with the previous (saved) value. If the values are equal this notification is issued again, signalling to the NMS that the condition has been cleared. Otherwise, the timer is restarted to monitor the next period.</p> <p>When a record is lost and no period timer is active, this notification is issued and the above procedure is repeated.</p> |
| ciscoCsgAgentStateChange        | <p>This notification is issued when <code>csgAgentNotifsEnabled</code> is set to 'true', and the billing mediation agent changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ciscoCsgQuotaMgrLostRecordEvent | <p>This notification is issued when <code>csgQuotaNotifsEnabled</code> is set to true, and the CSG must discard request records to be sent to the quota manager. The processing is the same as described in the description for <code>ciscoCsgAgentLostRecordEvent</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ciscoCsgQuotaMgrStateChange     | <p>This notification is issued when <code>csgQuotaNotifsEnabled</code> is set to true, and the quota manager changes state. There is one exception: No notification is issued for state changes involving <i>echowait</i> because this would cause an excessive number of notifications.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ciscoCsgUserDbStateChange       | <p>This notification is issued when <code>csgDatabaseNotifsEnabled</code> is set to true, and the user database changes state.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## CSG2 Traps

| Trap Name                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoContentServicesBMALostRecordEvent      | <p>This notification is issued when <code>ccsBMAShouldChangeNotifEnabled</code> is set to true, and accounting records, which should be sent to the billing mediation agent, must be discarded.</p> <p>Initially, <code>ccsBMALostRecords</code> is set to 0. When a record is discarded, <code>ccsBMALostRecords</code> is incremented, a period timer is started, and this notification is issued. The NMS and the agent save this value. The agent continues to increment <code>ccsBMALostRecords</code> each time a record is lost. When the period timer expires, the agent compares the current value of <code>ccsBMALostRecords</code> with the previous (saved) value. If the values are equal this notification is issued again, signalling to the NMS that the condition has been cleared. Otherwise, the timer is restarted to monitor the next period.</p> <p>When a record is lost and no period timer is active, this notification is issued and the above procedure is repeated.</p> |
| ciscoContentServicesBMAShouldChange         | <p>This notification is issued when <code>ccsBMAShouldChangeNotifEnabled</code> is set to true, and the billing mediation agent changes state. There is one exception: No notification is issued for state changes involving 'echowait' because this would cause an excessive number of notifications.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ciscoContentServicesQuotaMgrLostRecordEvent | <p>This notification is issued when <code>ccsQuotaMgrShouldChangeNotifEnabled</code> is set to true, and request records to be sent to the quota manager must be discarded. The processing is the same as described in the description for <code>ccsQuotaMgrLostRecordEvent</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| ciscoContentServicesQuotaMgrShouldChange    | <p>This notification is issued when <code>ccsQuotaMgrShouldChangeNotifEnabled</code> is set to true, and the quota manager changes state. There is one exception: No notification is issued for state changes involving <i>echowait</i> because this would cause an excessive number of notifications.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ciscoContentServicesUserDbShouldChange      | <p>This notification is issued when <code>ccsUserDbShouldChangeNotifEnabled</code> is set to true, and the user database changes state.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| cPsdClientDiskFullNotif                     | <p>This notification is generated when the PSD server's disk become full. If the disk of a writable PSD server becomes full, the client shall not be able to write any CDR into the server. It shall then behave as a retrieve only PSD server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Trap Name           | Description                                                                                                                                                                                          |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cPsdClientDownNotif | A notification of this type is generated when the PSD server goes DOWN.<br><br>If the PSD client was in write/retrieving state, then that operation shall be stopped.                                |
| cPsdClientUpNotif   | A notification of this type is generated when the PSD server comes UP.<br><br>A GTP' (GTP enhanced for charging) path will be created fulfilling all the specific requirements of the PSD interface. |

## GGSN Traps

| Trap Name                     | Description                                                                                                                                                                                                                                           |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cilpPercentAddrUsedHiNotif    | A notification indicating that the percentage of used addresses of an IP local pool is equal to or exceeds the threshold value indicated by cIpLocalPoolPercentAddrThldHi.                                                                            |
| cilpPercentAddrUsedLoNotif    | A notification indicating that the percentage of used addresses of an IP local pool went below the threshold value indicated by cIpLocalPoolPercentAddrThldLo.                                                                                        |
| ciscoIpLocalPoolInUseAddrNoti | A notification indicating that number of used addresses of an IP local pool exceeded the threshold value indicated by cIpLocalPoolStatInUseAddrThldHi.                                                                                                |
| cGgsnAccessPointNameNotif     | This notification indicates the occurrence of an APN (Access Point Name) related alarm.                                                                                                                                                               |
| cGgsnGlobalErrorNotif         | This notification indicates the occurrence of a GGSN related alarm.                                                                                                                                                                                   |
| cGgsnInServiceNotif           | A notification of this type is generated when GGSN is placed in inService mode, which is specified by cGgsnServiceModeStatus.                                                                                                                         |
| cGgsnMemThresholdClearedNotif | A notification of this type is generated when GGSN retains the memory and falls below threshold value specified by cGgsnMemoryThreshold.                                                                                                              |
| cGgsnMaintenanceNotif         | A notification of this type is generated when GGSN is placed in maintenance mode which is specified by cGgsnServiceModeStatus.                                                                                                                        |
| cGgsnMemThresholdReachedNotif | A notification of this type is generated when GGSN reaches the memory threshold value specified by cGgsnMemoryThreshold.                                                                                                                              |
| cGgsnNotification             | This notification indicates the occurrence of a GGSN related alarm. If and when additional useful information is available for specific types of alarms, then that information may be appended to the end of the notification in additional varbinds. |
| cGgsnPacketDataProtocolNotif  | This notification indicates the occurrence of a user related alarm.                                                                                                                                                                                   |
| cGgsnPdfStateDownNotif        | A notification of this type is generated when PDF (Policy Decision Function) connection goes DOWN.                                                                                                                                                    |
| cGgsnPdfStateUpNotif          | A notification of this type is generated when PDF connection comes UP.                                                                                                                                                                                |

| Trap Name                        | Description                                                                                                                                                                                                                                                                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cGgsnSACsgStateDownNotif         | This notification is generated when CSG state goes down.                                                                                                                                                                                                                                                                                 |
| cGgsnSACsgStateUpNotif           | This notification is generated when CSG state goes up.                                                                                                                                                                                                                                                                                   |
| cGgsnSADccaAuthRejectedNotif     | This notification is generated when credit-control server failed in authorization of end user. The PDP (Packet Data Protocol) context is deleted and category is blacklisted.                                                                                                                                                            |
| cGgsnSADccaCreditLimReachedNotif | This notification is generated when the credit limit is reached. The credit-control server denies the service request since the end user's account could not cover the requested service. Client shall behave exactly as with cGgsnSADccaEndUsrServDeniedNotif.                                                                          |
| cGgsnSADccaEndUsrServDeniedNotif | This notification is generated when the credit-control server denies the service request due to service restrictions. On reception of this notification on category level, the CLCI-C shall discard all future user traffic for that category on that PDP context and not attempt to ask for more quotas during the same PDP context.    |
| cGgsnSADccaRatingFailed          | This notification is generated when the credit-control server cannot rate the service request, due to insufficient rating input, incorrect AVP combination or due to an AVP (Attribute Value Pair) or an AVP value that is not recognized or supported in the rating.                                                                    |
| cGgsnSADccaUserUnknownNotif      | This notification is generated when the specified end user is unknown in the credit-control server. Such permanent failures cause the client to enter the Idle state. The client shall reject or terminate the PDP context depending on whether the result code was received in a CCA (Credit Control Answer) (Initial) or CCA (Update). |
| cGtpPathFailedNotification       | This notification is sent when one of this GSN's peers failed to respond to the GTP (GPRS Tunneling Protocol) Echo Request message for the waiting interval.                                                                                                                                                                             |
| cPsdClientDiskFullNotif          | A notification of this type is generated when the PSD (Persistent Storage Device) server's disk become full.<br><br>If the disk of writable PSD server becomes full, the client shall not be able to write any CDR into the server. It shall then behave as a retrieve only PSD server.                                                  |
| cPsdClientDownNotif              | A notification of this type is generated when the PSD server goes DOWN.<br><br>If the PSD client was in write/retrieving state, then that operation shall be be stopped.                                                                                                                                                                 |
| cPsdClientUpNotif                | A notification of this type is generated when the PSD server comes UP.<br><br>A GTP' (GTP enhanced for charging) path will be created fulfilling all the specific requirements of the PSD interface.                                                                                                                                     |
| cgprsAccPtCfgNotif               | A notification of this type is generated when an entry is generated in the cgprsAccPtCfgNotifHistTable and cgprsAccPtCfgNotifEnable is set to true.                                                                                                                                                                                      |
| cgprsAccPtInServiceNotif         | A notification of this type is generated when APN is placed in in-service mode which is specified by cgprsAccPtOperationMode.                                                                                                                                                                                                            |

| Trap Name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cgprsAccPtMaintenanceNotif    | A notification of this type is generated when APN is placed in maintenance mode which is specified by cgprsAccPtOperationMode.                                                                                                                                                                                                                                                                                                         |
| cgprsAccPtSecDestViolNotif    | A notification of this type is generated when security violation as specified by cgprsAccPtVerifyUpStrTpduDstAddr occurs on an APN.                                                                                                                                                                                                                                                                                                    |
| cgprsAccPtSecSrcViolNotif     | A notification of this type is generated when security violation as specified by cgprsAccPtVerifyUpStrTpduSrcAddr occurs on an APN.                                                                                                                                                                                                                                                                                                    |
| cgprsCgAlarmNotif             | A cgprsCgAlarmNotif signifies that a GPRS (General Packet Radio Service) related alarm is detected in the managed system. This alarm is sent after an entry has been added to cgprsCgAlarmHistTable.                                                                                                                                                                                                                                   |
| cgprsCgGatewaySwitchoverNotif | <p>A notification of this type is generated when the charging gateway is switched, the new charging gateway is identified by cgprsCgActiveChgGatewayAddress and the old charging gateway is identified by cgprsCgOldChgGatewayAddress.</p> <p>The switchover will happen according to the value set in cgprsCgGroupSwitchOverTime and the selection of the new CG will be according to the value set in cgprsCgSwitchOverPriority.</p> |
| cgprsCgInServiceModeNotif     | A notification of this type is generated when the GGSN charging function is in normal mode. This can be identified by cgprsCgServiceMode object.                                                                                                                                                                                                                                                                                       |
| cgprsCgInServiceModeNotif     | A notification of this type is generated when the GGSN charging function is in normal mode. This can be identified by cgprsCgServiceMode object.                                                                                                                                                                                                                                                                                       |
| cgprsCgMaintenanceModeNotif   | A notification of this type is generated when the GGSN charging function is in maintenance mode. This can be identified by cgprsCgServiceMode object.                                                                                                                                                                                                                                                                                  |

## BWG Traps

| Trap Name                                | Description                                                                                                                                                                                                  |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ciscoAgwMaxBaseStationExceededAbateNotif | A notification of this type is generated when the number of base stations goes below the percent of the maximum number of base stations as specified by the object cagwMaxBaseStationExceededNotifThreshold. |
| ciscoAgwMaxBaseStationExceededOnsetNotif | A notification of this type is generated when the number of base stations exceeded the percent of the maximum number of base stations as specified by the object cagwMaxBaseStationExceededNotifThreshold.   |
| ciscoAgwMaxSubscribersExceededAbateNotif | A notification of this type is generated when the number of subscribers goes below the percent of the maximum number of base stations as specified by the object cagwMaxSubscribersExceededNotifThreshold.   |
| ciscoAgwMaxSubscribersExceededOnsetNotif | A notification of this type is generated when the number of subscribers exceeded the percent of the maximum number of base stations as specified by the object cagwMaxSubscribersExceededNotifThreshold.     |
| ciscoAgwServiceDownNotif                 | A notification of this type is generated when the BWG is not in service.                                                                                                                                     |
| ciscoAgwServiceUpNotif                   | A notification of this type is generated when the BWG is in service.                                                                                                                                         |

## HA Traps

| Trap Name                      | Description                                                                                                                                                                |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cilpPercentAddrUsedHiNotif     | A notification indicating that the percentage of used addresses of an IP local pool is equal to or exceeds the threshold value indicated by cIpLocalPoolPercentAddrThldHi. |
| cilpPercentAddrUsedLoNotif     | A notification indicating that the percentage of used addresses of an IP local pool went below the threshold value indicated by cIpLocalPoolPercentAddrThldLo.             |
| ciscoIpLocalPoolInUseAddrNotif | A notification indicating that number of used addresses of an IP local pool exceeded the threshold value indicated by cIpLocalPoolStatInUseAddrThldHi.                     |
| cmiHaMnRegReqFailed            | The Mobile Node (MN) registration request failed notification. This notification is sent when the registration request from MN is rejected by the HA.                      |
| cmiHaMaxBindingsNotif          | The HA total registrations reached maximum bindings. This notification is sent when the registration request from MN is rejected by the HA.                                |
| mipAuthFailure                 | Indicates that the Mobile IP entity has an authentication failure when it validates the mobile Registration Request or Reply.                                              |







## APPENDIX **H**

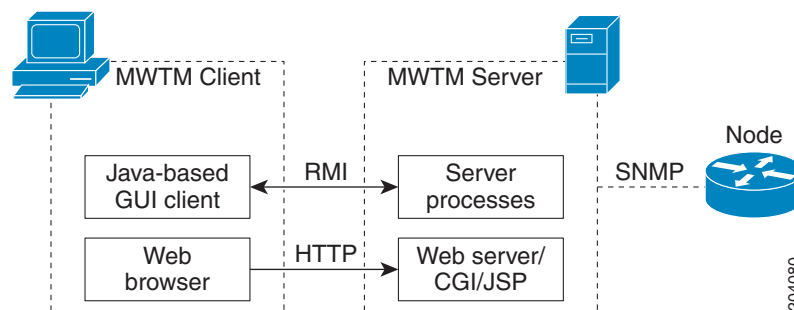
# Configuring MWTM to Run with Various Networking Options

In addition to running on standard IP-connected networks, the Cisco Mobile Wireless Transport Manager (MWTM) has the flexibility to adapt to a variety of different networking environments, including Virtual Private Network (VPN), Network Address Translation (NAT), firewall, port-forwarding, and Secure Sockets Layer (SSL). The MWTM software can run in each of these environments individually, or in any combination of networking environments.

This appendix describes communication between the MWTM client and the MWTM server. [Figure H-2](#) includes the following:

- Two-way Remote Method Invocation (RMI) communication between a Java-based GUI client and Java-based server processes. The client can send requests to and receive responses from the server, and the server can send unsolicited notifications to the client. For example, if the server detects that an ITP's state has changed, it sends a notification to all MWTM clients to update their topology windows.
- One-way HTTP communication between a web browser and an MWTM-embedded web server, using the request/response model.

**Figure H-1** *MWTM Communication*



The diagram illustrates the MWTM architecture. On the left, the **MWTM Client** is represented by a stack of blue computer icons. It contains two components: a **Java-based GUI client** and a **Web browser**. On the right, the **MWTM Server** is represented by a blue server rack icon. It contains two components: **Server processes** and a **Web server/CGI/JSP**. A **Node**, represented by a blue circular icon with arrows, is connected to the MWTM Server. The connections are as follows: a double-headed arrow labeled **RMI** connects the Java-based GUI client to the Server processes; a single-headed arrow labeled **HTTP** connects the Web browser to the Web server/CGI/JSP; and a dashed line labeled **SNMP** connects the MWTM Server to the Node.



### Note

This appendix does not address communication between the MWTM server and the ITP, which uses the SNMP protocol for network management.

This appendix contains:

- [How Does RMI Work?, page H-2](#)
- [VPN Communication, page H-3](#)
- [NAT Communication, page H-5](#)
- [Firewall Communication, page H-6](#)
- [Port-Forwarding Communication, page H-12](#)
- [Configuring MWTM to Work With a Dual-Interface Machine Connected to Separate Networks, page H-14](#)
- [Additional Network Configurations, page H-17](#)
- [Configuring MWTM with IOS Server Load Balancing, page H-18](#)

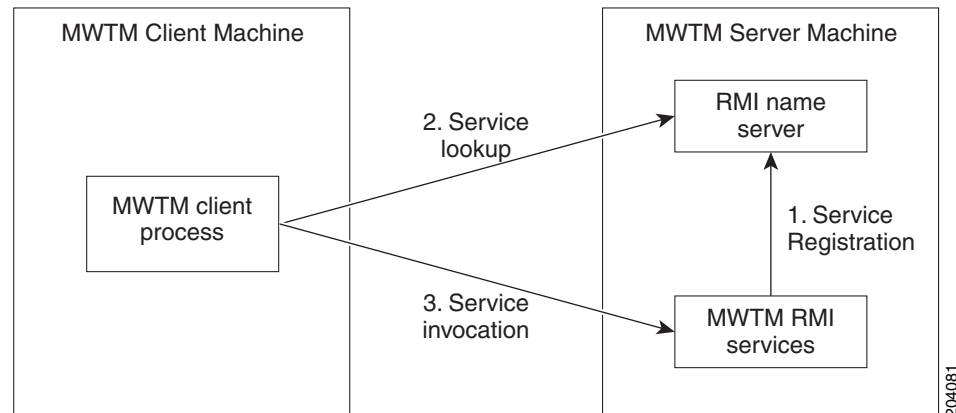
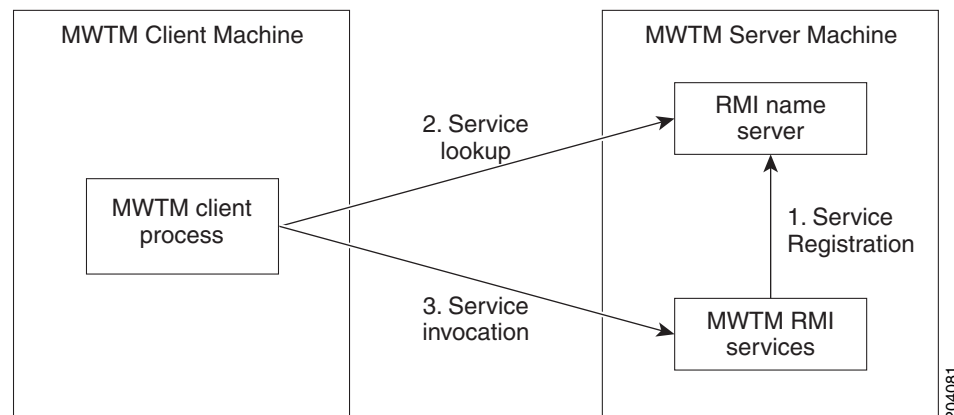
## How Does RMI Work?

RMI is a Java-based technology that allows a Java application to communicate with another Java application (usually residing on different hosts) using remote method invocation. RMI marshals and unmarshals method parameters and return values using Java object serialization. It uses TCP connections as the default communication mechanism.

Understanding how RMI works can assist your understanding of the different scenarios presented in this appendix.

Three types of RMI components exist between the MWTM client and server communication:

- **RMI name server**—Runs on the MWTM server
- **MWTM RMI services**—Runs on the MWTM server
- **MWTM client process**—Runs on the MWTM client

**Figure H-3 RMI Components****Figure H-4 RMI Components**

When the MWTM server starts, the MWTM RMI services register with the RMI name server. These registered RMI services have one single published IP address.

When the MWTM client starts, it first establishes a TCP connection to the RMI name server and performs a service lookup. The RMI name server returns the published IP address for the MWTM RMI services. The MWTM client then establishes another TCP connection to the published IP address of the MWTM RMI services for client and server communication.

This appendix describes how to configure the MWTM software to adjust the communication process outlined previously, in order to make the MWTM work with NAT, Port-Forwarding, and/or a Dual-Interface MWTM server.

## VPN Communication



### Note

VPN configuration is transparent to the user; no manual configuration is needed.

MWTM client/server communication can run transparently through a VPN tunnel, which is a secure IP layer, without any user intervention. You can use VPN to connect to a corporate network, then start the MWTM client to connect through the VPN tunnel to an MWTM server in the corporate network.

When the client host establishes a VPN tunnel, the operating system (or system library) sees this as another virtual IP interface. The VPN tunnel does not affect HTTP communication between the web browser and server, it only affects RMI communication between the MWTM client and server processes.

For HTTP communication, the virtual IP address is transparent to the upper layer. The operating system automatically chooses the correct IP address to send out the request packet. For RMI communication, the MWTM client must register with the MWTM server using the correct IP address, so that the server can invoke RMI callbacks and send unsolicited notifications to the client.

The MWTM software solves this problem by automatically detecting the local IP interface so that the MWTM server can send unsolicited notification to the correct IP address.

Figure H-6 shows a sample VPN network with these characteristics:

- The MWTM client with IP address 192.168.0.1 is connected to the MWTM server network through a VPN tunnel.
- The MWTM client host has obtained VPN IP address 10.1.1.2, which is a virtual IP interface.

**Figure H-5 VPN Communication**

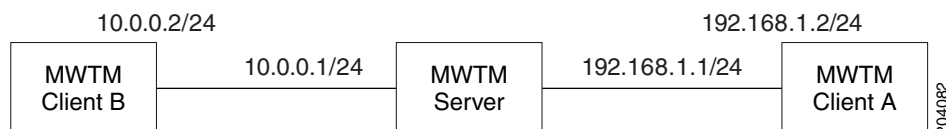
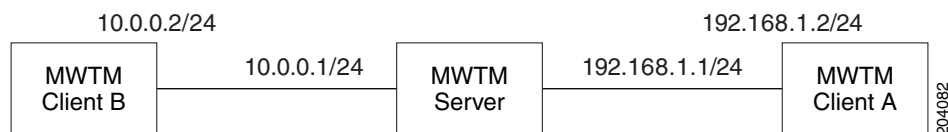


**Figure H-6 VPN Communication**



When connecting to the MWTM server, the MWTM client automatically recognizes its VPN IP address, 10.1.1.2, and uses that address to register with the MWTM server to receive RMI callbacks.

# NAT Communication

MWTM client/server communication can run through one or more static NAT-connected networks.



## Note

The MWTM software does not support dynamic NAT or dynamic NAT pool overloading.

In a static NAT network, the MWTM client and server reside on different sides of the NAT network, with no routes between the client network and the server network. The NAT device statically maps the client IP address to a NAT address in the server network, and the server IP address to a NAT address in the client network.

The NAT device translates packets between the MWTM client and server by replacing IP address headers when packets pass through. From the client's point of view, the server appears to be at a NAT IP address in the client network, and vice versa. For most protocols, this technique is sufficient to enable the client and server to communicate.

However, for the RMI protocol, this is not sufficient. The RMI protocol requires the client and server to keep remote object references by remote stubs. These remote stubs contain the remote objects' IP addresses, and are passed between the client and server using Java serialization. The NAT device only converts the IP addresses in the IP packet header, but the remote stub object is in the packet content. Therefore, the NAT device cannot recognize the IP address inside the packet, and fails to route it correctly.

The MWTM software solves this problem by creating a specialized NAT-aware socket factory. The user must perform some manual configuration to enable the MWTM to “know” the network NAT configuration.

Figure H-8 shows a sample static NAT network with these characteristics:

- A static NAT device connects Network A (192.168.\*.\*) to Network B (10.\*.\*.\*), with no routes between Network A and Network B.
- The NAT device maps the MWTM client IP address 192.168.0.1 in Network A to 10.1.1.2 in Network B.
- The NAT device maps the MWTM server IP address 10.0.0.1 in Network B to 192.168.1.2 in Network A.

**Figure H-7 Static NAT Communication**

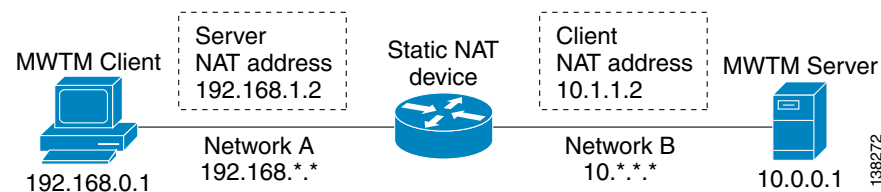
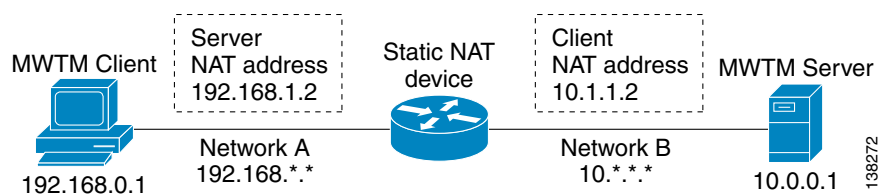


**Figure H-8 Static NAT Communication**

To configure the MWTM software in this static NAT network, you must change the MWTM client's *RMIOverNAT.properties* file.

- In Solaris/Linux, if you installed the MWTM software in the default directory, */opt*, then the location of the file is */opt/CSCOsgmClient/properties/RMIOverNAT.properties*.
- In Windows, if you installed the MWTM software in the default directory, *C:\Program Files*, then the location of the file is *C:\Program Files\SGMClient\properties\RMIOverNAT.properties*.
- If you installed the MWTM software in a different directory, then the file resides in that directory.

For the example shown in [Figure H-8](#), you must add this line to the file:

```
10.0.0.1 = 192.168.1.2
```

This line maps the MWTM server's real IP address, 10.0.0.1 in Network B, to its NAT address, 192.168.1.2, in Network A, which is the server's IP address as seen by the client.

**Note**

The MWTM server automatically detects the MWTM client's NAT address. No manual configuration on the part of the user is needed at the server side.

When the MWTM server starts, it starts MWTM services that register with the RMI server and publish themselves with the IP address specified in the *SERVER\_NAME* property of *System.properties* file on the MWTM server. In the given example, the published IP address is 10.0.0.1.

The MWTM client starts and connects to 192.168.1.2 (specified as the MWTM client's default server address). The NAT device translates the MWTM client's request to the RMI server at 10.0.0.1.

The MWTM client then asks where the MWTM services are located. The RMI server replies that these MWTM services reside at 10.0.0.1. Without the *RMIOverNAT.properties* file on the MWTM client, the client will try to connect to 10.0.0.1, which would fail.

If we have configured the *RMIOverNAT.properties* file on the MWTM client as in the example, the MWTM client will still connect to 192.168.1.2 for name lookup, and the name server will return that MWTM services are running on 10.0.0.1. The MWTM client then looks in the *RMIOverNAT.properties* file, and discovers that the translated address for 10.0.0.1 is 192.168.1.2. With this configuration, the MWTM client will try to connect to 192.168.1.2 for RMI services (instead of 10.0.0.1). As the result, the connection will be established successfully.

## Firewall Communication

To enable MWTM client/server communication through a firewall, you need to set up the firewall so that it allows MWTM communication packets to pass through freely.

This section contains:

- [Configuring Port Numbers and Parameters, page H-7](#)

- [Configuring Firewalls, page H-8](#)
- [Sample Firewall Configuration, page H-10](#)

## Configuring Port Numbers and Parameters

**Note**

The MWTM client and server communicate using TCP sockets. All port numbers in this section are TCP ports.

The port number used by the MWTM software is configured in the *System.properties* file:

- If you installed the MWTM software in the default directory, */opt*, then the location of the file is */opt/CSCOsgm/properties/System.properties*.
- In Windows, if you installed the MWTM software in the default directory, *C:\Program Files*, then the location of the file is *C:\Program Files\SGMClient\properties\System.properties*.
- If you installed the MWTM software in a different directory, then the file resides in that directory.

Set these parameters on the *server* side of the file:

RMIREGISTRY\_PORT = 44742

DATASERVER\_PORT = 0

LOGINSERVER\_PORT = 0

WEB\_PORT = 1744

where:

- RMIREGISTRY\_PORT is the port on which the RMI naming server listens. You must specify a port number; **0** is not allowed.
- DATASERVER\_PORT is the port on which the Data Service listens. If you specify **0**, the MWTM software uses a random available port, 1024 and above. The MWTM maintains the chosen port until the next server restart.
- LOGINSERVER\_PORT is the port on which the Log in Service listens. If you specify **0**, the MWTM software uses a random available port, 1024 and above. The MWTM maintains the chosen port until the next server restart.
- WEB\_PORT is the port on which the MWTM web server listens. You must specify a port number; **0** is not allowed. To change the WEB\_PORT number, use the **mwtm webport** command (see [mwtm webport, page B-83](#)).

**Note**

If any of these port numbers change, you must restart the MWTM server before the changes take effect.

Set these parameters in the MWTM *client's* *System.properties* file:

RMIREGISTRY\_PORT = 44742

CLIENT\_PORT = 0

where:

- RMIREGISTRY\_PORT is the port on which the server-side RMI naming server listens. This port number must match the one specified for the RMIREGISTRY\_PORT on the server side.

- CLIENT\_PORT is the port on which the MWTM client listens for RMI callbacks (unsolicited notifications):
  - If you specify CLIENT\_PORT = 0, the MWTM software uses any available port, 1024 and above.
  - If you specify CLIENT\_PORT with a single value other than 0, such as CLIENT\_PORT = 33459, the MWTM software uses that port, and you can run only one MWTM client process at a time.
  - If you specify CLIENT\_PORT with a range of values other than 0, such as CLIENT\_PORT = 33459-33479, the MWTM software can use any of the ports in the range, including the beginning and ending ports, and you can run more than one MWTM client process at a time.

**Note**

If any of these port numbers change, you must restart the MWTM client before the changes take effect.

The MWTM client's *System.properties* file resides in the *properties* directory:

- In Solaris/Linux, if you installed the MWTM software in the default directory, */opt*, then the location of the file is */opt/CSCOsgmClient/properties/System.properties*.
- In Windows, if you installed the MWTM software in the default directory, *C:\Program Files*, then the location of the file is *C:\Program Files\SGMClient\properties\System.properties*.
- If you installed the MWTM software in a different directory, then the file resides in that directory.

## Configuring Firewalls

**Step 1** Identify the TCP port numbers to use between the MWTM server and client applications.

The MWTM software uses four TCP port numbers on the server side and two TCP port numbers on the client side to communicate between the MWTM server and client(s). These ports include the RMI Registry Port, the Data Server Port, the Login Server Port, the Client Port, and the HTTP Web Server port.

These ports are used for two way TCP connections between the MWTM server and client as follows:

1. For a client initiating a connection to the server, the initiating port on the client side is dynamic, and the target port on the server can be fixed by the DATASERVER\_PORT and LOGINSERVER\_PORT properties on the server.
2. For the server initiating a connection to the client (this is used for status change notifications), the initiating port on the server side is dynamic, and the target port on the client can be fixed by the CLIENT\_PORT property on the client side.

You configure these port numbers in a plain-text file named *System.properties* located on the MWTM server and client. When configuring the MWTM software in a firewall deployment, you should use these port numbers:

- **RMI Registry Port**—44742
- **Data Server Port**—44751
- **Login Server Port**—44752
- **Client Port**—56173
- **HTTP Web Server Port**—1774



- Step 2** Modify the *System.properties* file on the MWTM server. The *System.properties* file resides on the MWTM server under the */opt/CSCOsgm/properties* directory.



**Note** If the you installed the MWTM software in a location other than the default (*/opt/CSCOsgm*), substitute the correct directory name to locate the properties directory.



**Caution** Before editing, always make a backup of the file. This ensures a valid file exists in case an error is made during the editing process.

Using a text editor, edit this file and specify the appropriate port number where indicated subsequently:

| Port Name            | Keyword          | Value |
|----------------------|------------------|-------|
| RMI Registry Port    | RMIREGISTRY_PORT | 44742 |
| Data Server Port     | DATASERVER_PORT  | 44751 |
| Login Server Port    | LOGINSERVER_PORT | 44752 |
| HTTP Web Server Port | WEB_PORT         | 1774  |

- Step 3** Modify the *System.properties* file on the MWTM client. The *System.properties* file resides on the MWTM client machine under:

- */opt/CSCOsgm/properties* directory for Solaris clients
- *C:\Program Files\MWTMClient\properties* for Windows clients



**Note** If the you installed the MWTM software in a location other than the default (*/opt/CSCOsgmClient*), substitute the correct directory name to locate the properties directory.



**Caution** Before editing, always make a backup of the file. This ensures a valid file exists in case an error is made during the editing process.

Using a text editor, edit this file and specify the appropriate port number where indicated subsequently:

| Port Name         | Keyword          | Value |
|-------------------|------------------|-------|
| RMI Registry Port | RMIREGISTRY_PORT | 44742 |
| Client Port       | CLIENT_PORT      | 56173 |

- Step 4** Modify the node configuration files with the chosen port numbers.

On Cisco nodes, you can use extended access lists to allow the chosen TCP port numbers to pass between the appropriate interface(s). Assuming a single node separates the MWTM client and server, you can use the following extended access list:

**Note**

The *established* entries are necessary, as they allow data to flow between the server and client that initiated the session. Without this keyword, clients will not have access to the MWTM server.

```
MWTM Client Interface
interface FastEthernet 1/1
 ip address 192.168.1.100 255.255.255.0
 ip access-group client-to-server in

MWTM Server Interface
interface FastEthernet 2/1
 ip address 192.168.2.100 255.255.255.0
 ip access-group server-to-client in

Access list from client to server
ip access-list extended client-to-server
 10 permit tcp any any established
 20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44742
 30 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44751
 40 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44752
 50 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 1774

Access list from server to client
ip access list extended server-to-client
 10 permit tcp any established
 20 permit tcp host 192.168.2.2 192.168.1.0 0.0.0.255 eq 56173
```

**Step 5** Restart the MWTM server to use the newly chosen TCP port numbers.

As the root user, on the MWTM server, type:

```
#/opt/CSCOsrgm/bin
#./mwtm restart
```

The server processes restart using the newly chosen port numbers.

## Sample Firewall Configuration

This sample shows how to configure your firewall from the server side, client side, and Cisco node side.

[Figure H-10](#) shows a sample firewall network with these parameters set in the *System.properties* file:

- On the MWTM server side:
  - RMIREGISTRY\_PORT = 44742
  - DATASERVER\_PORT = 44751
  - LOGINSERVER\_PORT = 44752
  - WEB\_PORT = 1774
- On the MWTM client side:
  - RMIREGISTRY\_PORT = 44742
  - CLIENT\_PORT = 56173

**Figure H-9 Firewall Communication**

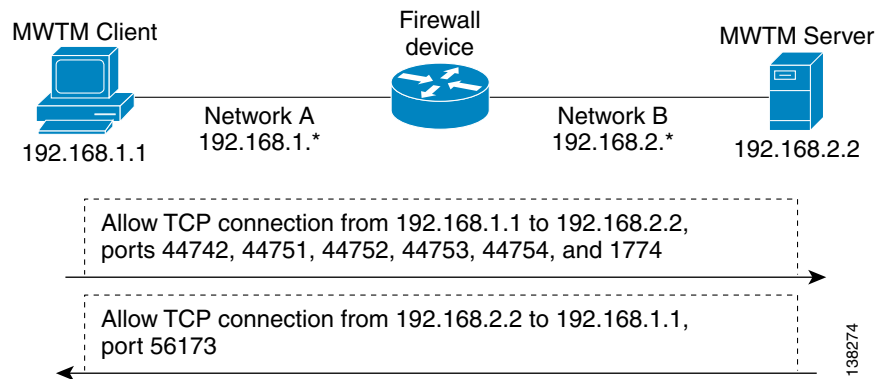
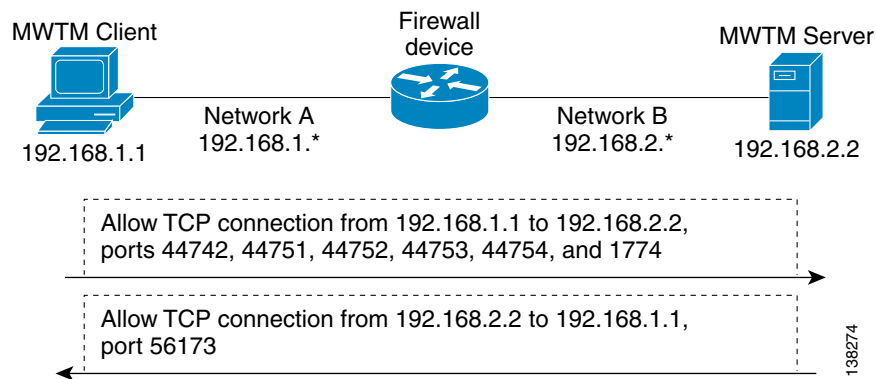


**Figure H-10 Firewall Communication**



This example illustrates a typical firewall configuration for Cisco nodes using access lists. This examples has two extended access lists:

- **ip access-list extended client-to-server**—This access list is applied on the input interface from the client to the server (FE 1/1).
- **ip access-list extended server-to-client**—This access list is applied on the input interface from the server to the client (FE 2/1).

```
!
ip access-list extended client-to-server
 10 permit tcp any any established
 20 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44742
 30 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44751
 40 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 44752
 50 permit tcp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq 1774
 60 ...
!
ip access list extended server-to-client
 10 permit tcp any any established
 20 permit tcp host 192.168.2.2 192.168.1.0 0.0.0.255 eq 56173
 30 ...
!
interface FastEthernet 1/1
 ip address 192.168.1.100 255.255.255.0
 ip access-group client-to-server in
!
!
interface FastEthernet 2/1
 ip address 192.168.2.100 255.255.255.0
 ip access-group server-to-client in
!
!
!
```



#### Note

Both of these access lists allow established TCP connections (*10 permit tcp any any established, see previous*). When the MWTM client or server establishes a TCP connection to the other end, it uses a fixed destination port. However, the source port from the initiating party is random. The established keyword allows a returning TCP packet to go back to the random initiating source port.

## Port-Forwarding Communication

To enable the MWTM software to operate in a TCP port-forwarding environment, perform these configuration tasks:

- 
- Step 1** Configure the server hostname and port number mapping in the MWTM client's *RMIOverNAT.properties* file, as described in [NAT Communication, page H-5](#).
  - Step 2** Configure the port numbers used by the MWTM client and server in the *System.properties* file, as described in [Firewall Communication, page H-6](#).
  - Step 3** Configure the port-forwarding tunnel to forward each side's TCP connection to the other side.
-

Figure H-12 shows a sample network that uses Secure Shell (SSH) port-forwarding. Other port-forwarding configurations might use a single host with dual interfaces at the client's and server's networks. While other port-forwarding configurations might differ from this example, the general rules to configure the MWTM software to operate in a port-forwarding environment are the same.

**Figure H-11** Port-Forwarding Communication

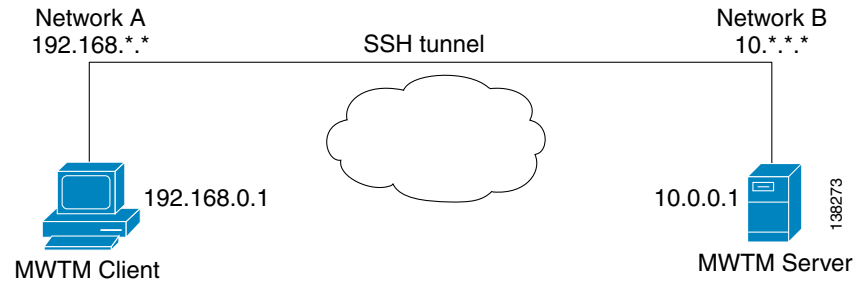
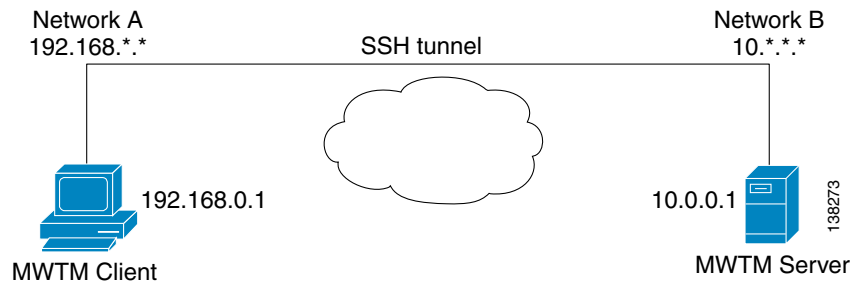


**Figure H-12** Port-Forwarding Communication



The port-forwarding network shown in Figure H-12 has these parameters set:

- In the *System.properties* file, on the MWTM server side:  
`RMIREGISTRY_PORT = 44742`  
`DATASERVER_PORT = 44751`  
`LOGINSERVER_PORT = 44752`  
`WEB_PORT = 1774`
- In the *System.properties* file, on the MWTM client side:  
`RMIREGISTRY_PORT = 44742`  
`CLIENT_PORT = 56173`
- In the MWTM client's *RMIOverNAT.properties* file:  
`10.0.0.1/44742 = 127.0.0.1/25742`  
`10.0.0.1/44751 = 127.0.0.1/25751`  
`10.0.0.1/44752 = 127.0.0.1/25752`  
`10.0.0.1/1774 = 127.0.0.1/8080`
- In the port-forwarding network:  
`Local port 25751 => remote host 127.0.0.1, port 44742`

Local port 25751 => remote host 127.0.0.1, port 44751

Local port 25752 => remote host 127.0.0.1, port 44752

Local port 8080 => remote host 127.0.0.1, port 1774

Remote port 56173 => local host 127.0.0.1, port 56173



**Note**

For port-forwarding setup, the backward-forwarding port numbers must match each other. In the previous example, both are 56173. The forward-forwarding port numbers do not need to match each other.

If you want to run more than one MWTM client process at the same time on the same node, you must specify `CLIENT_PORT` with a range of values other than 0, such as `CLIENT_PORT = 33459-33479`, in the MWTM client's *RMIOverNAT.properties* file. See [Firewall Communication, page H-6](#) for more information about specifying the `CLIENT_PORT` parameter. You must also set up the backward-forwarding port numbers to use a range of values.

When the MWTM server starts, underlying network services register with the RMI server and publish themselves with the IP address specified in the `SERVER_NAME` property of the *System.properties* file on the MWTM server. In the given example, the published IP address is 10.0.0.1.

The MWTM client starts and connects to the localhost/127.0.0.1 (specified as the MWTM client's default server address). The SSH port-forwarding tunnel forwards the MWTM client's request to the RMI server at the MWTM server's localhost/127.0.0.1.

The MWTM client then asks where the MWTM services are located, and the RMI server replies that these MWTM services reside at 10.0.0.1. Without the *RMIOverNAT.properties* file on the MWTM client, the client would try to connect to 10.0.0.1, which would fail because of a network routing problem.

If we have configured the *RMIOverNAT.properties* file on the MWTM client as in the example, the MWTM client will still connect to the localhost/127.0.0.1 for name lookup, and the name server would return that MWTM services are running on 10.0.0.1. The MWTM client then looks in the *RMIOverNAT.properties* file, and discovers that the translated address for 10.0.0.1 is 127.0.0.1. With this configuration, the MWTM client will try to connect to 127.0.0.1 for RMI services (instead of 10.0.0.1). As a result, the connection will establish successfully.

## Configuring MWTM to Work With a Dual-Interface Machine Connected to Separate Networks

The MWTM client and server communication is based on Java RMI protocol. A limitation of RMI is its inability to publish itself with more than one specific IP address. This means that the RMI service can only register to one single interface on a dual interface machine. You can deploy the MWTM server on a dual interface machine in various scenarios:

- In some scenarios, all MWTM clients run on one side of the MWTM server interface, with no MWTM clients on the other side of the interface (for example, the other MWTM server interface is exclusively used for network management/SNMP traffic). In this scenario, ensure that the MWTM server published address is the interface connected to the MWTM clients. To change the published address of the MWTM server, see [mwtm servername, page B-57](#).

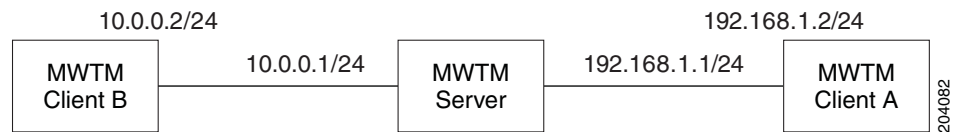
- In some other scenarios, the two MWTM server interfaces are connected to the same network, or the two interfaces are connected to two different networks, but these networks are routed between each other. Typically, the intention is to use two physical interfaces to provide redundancy on the MWTM server. When providing physical interface redundancy, you should use Cisco Server Load Balancing technology. For details on configuring the MWTM software with this scenario, see [Configuring MWTM with IOS Server Load Balancing, page H-18](#).

This section describes a third scenario: how to configure the MWTM software to work with a dual-interface machine that is connected to two separate networks. Both networks have MWTM clients that need to connect to the MWTM server. [Figure H-14](#) is a diagram of a sample network where a single MWTM server is connected to two separate networks. Two MWTM clients, A and B, are on these two separate networks and need to communicate with the MWTM server.

**Figure H-13 Sample Network**



**Figure H-14 Sample Network**



In this network configuration, the two networks (192.168.1.0/24 and 10.0.0.0/24) are not routed between each other. If the two networks were routed between each other (for example, if MWTM client B at 10.0.0.2 could reach the MWTM server at 192.168.1.1), you would configure the MWTM server with the 192.168.1.1 address, which would enable MWTM client A and MWTM client B to connect to the MWTM server.

The following sections give an example of how to configure the MWTM software to work with MWTM clients on both networks.

## MWTM Server Configuration

The MWTM server can publish only one single IP address on the MWTM server machine. To configure this published address, use the **mwtm servername** command (see [mwtm servername, page B-57](#)).

For example, a system administrator configures the MWTM server to use the 192.168.1.1 address, by running the command **mwtm servername 192.168.1.1** on the MWTM server machine. The MWTM server will restart for the change to take effect. The command changes the *System.properties* file on the MWTM server to contain following line:

```
SERVER_NAME = 192.168.1.1
```

## MWTM Client A Configuration

No special configurations are required on MWTM client A. Because this client is on the same network as the MWTM server binding interface, MWTM client A can communicate freely with the MWTM server.

You do need to ensure that during installation, MWTM client A has set up the MWTM server IP address as 192.168.1.1.

If the initial installation has incorrect information, you can change the MWTM server IP address to 192.168.1.1 using the **mwtm servername** command, or you can use the Change Default MWTM Server option on the MWTM client menu. For detailed information, see [mwtm servername](#), page B-57, or [Changing the Default MWTM Server Name](#), page 4-31.

## MWTM Client B Configuration

When the MWTM server starts up on a dual-interface machine, it starts the RMI server and binds it to all the interfaces.

The MWTM server then starts all MWTM services and binds them to all the interfaces. These MWTM services then register with the RMI server and publish themselves with the IP address specified in the `SERVER_NAME` property of the `System.properties` file on the MWTM server. In the given example, the published IP address is 192.168.1.1.

MWTM client B starts up, connecting to 10.0.0.1 (specified as the MWTM client B default server address). MWTM client B connects to the RMI server at 10.0.0.1.

MWTM client B then asks where the MWTM services are located. The RMI server replies that these MWTM services reside at 192.168.1.1. Without the `RMIOverNAT.properties` file on the MWTM client B, the client would try to connect to 192.168.1.1, which would fail.

If we have configured the `RMIOverNAT.properties` file on MWTM client B as in the example, MWTM client B will still connect to 10.0.0.1 for name lookup, and the name server will return that MWTM services are running on 192.168.1.1. The MWTM client then looks in the `RMIOverNAT.properties` file, and discovers that the translated address for 192.168.1.1 is 10.0.0.1. With this configuration, MWTM client B will try to connect to 10.0.0.1 (instead of 192.168.1.1) for RMI services. As the result, the connection will establish successfully.

Configuring MWTM client B involves two things:

- First, ensure that MWTM client B has setup the MWTM server IP address as 10.0.0.1 during installation.  
  
If the initial installation has incorrect information, you can also change the MWTM server IP address to 10.0.0.1 using the **mwtm servername 10.0.0.1** command, or using the Change Default MWTM Server option on the MWTM client menu.
- Next, you must edit the `RMIOverNAT.properties` file on the MWTM client machine. On a Windows client, the default location of this file is `C:/ProgramFiles/SGMClient/properties/RMIOverNAT.properties`. On a Solaris client, the default location of this file is `/opt/CSCOmwcClient/properties/RMIOverNAT.properties`.

Add this line in the `RMIOverNAT.properties` file:

```
192.168.1.1 = 10.0.0.1
```

After you have completed these steps, MWTM client B will be able to connect to the MWTM server even if the MWTM server published address 192.168.1.1 is unreachable from MWTM client B. MWTM client B will convert 192.168.1.1 to a reachable IP address 10.0.0.1 for client to server TCP connection.



## Additional Network Configurations

Numerous other network configurations are not directly addressed here. The MWTM client and server can work with most of these networks, as long as the MWTM client and server can establish an SSH connection.

A few examples of alternative network configurations are:

- Dynamic NAT, where the MWTM client and server are on two different sides of the dynamic NAT network.
- A situation where the MWTM client is in a trusted network and the MWTM server is in a public network, but the firewall does not allow a direct TCP connection made from the MWTM server to the MWTM client.
- A situation where the MWTM server is in a trusted network and the MWTM client is in a public network, but the firewall does not allow a direct TCP connection made from MWTM client to MWTM server.

To allow the MWTM client and server communication in these network environments, you can establish a SSH connection between the MWTM client and the MWTM server using SSH port-forwarding (for details, see [Port-Forwarding Communication, page H-12](#)).

## SSL Communication

If SSL is implemented and enabled in your MWTM system, the MWTM software uses secure socket communication for both RMI and HTTP communication between the MWTM client and server.

The MWTM software supports standard-based SSL encryption algorithms, including RSA, DSA public key algorithms, and 40-bit or 128-bit encryption. The MWTM software can generate an X.509 certificate and a certificate signing request (CSR), which is interoperable with most certificate authorities (CAs).

Both the MWTM web server and the MWTM server processes share the same SSL key/certificate pair. In addition, the MWTM client and the web browser can examine the server's certificate.

For more information, including descriptions of the MWTM commands and procedures used to implement, enable, manage, and monitor SSL support, see [Implementing SSL Support in the MWTM, page 2-22](#).

[Figure H-16](#) shows a sample MWTM-over-SSL network with these characteristics:

- A user-generated SSL key pair on the MWTM server.
- The server's certificate is trusted on the MWTM client.
- Communication between the client and server is RMI-over-SSL and HTTPS. Both protocols are encrypted and secure.

Figure H-15 SSL Communication

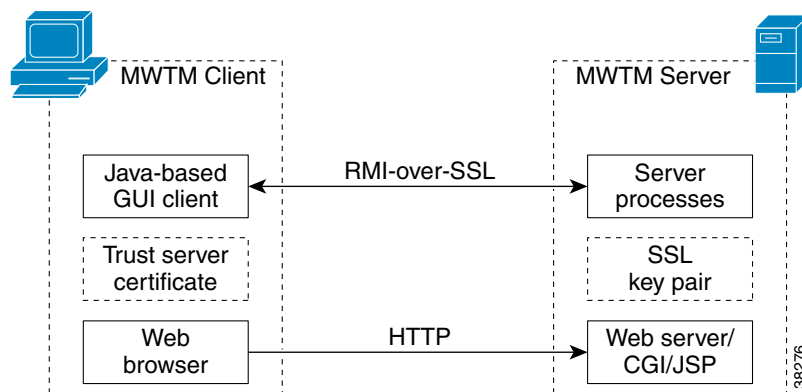
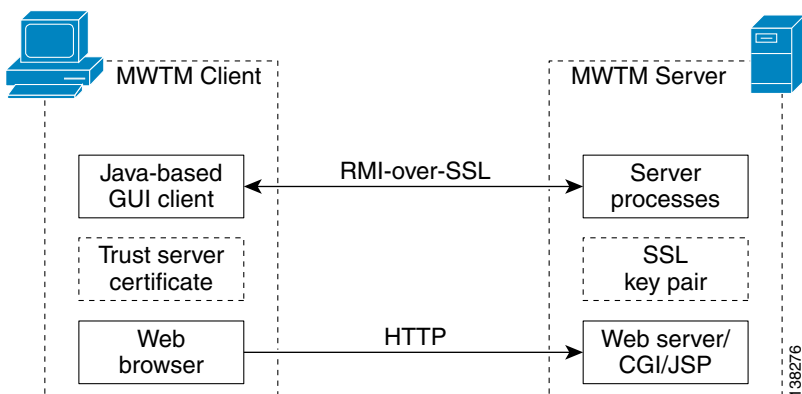


Figure H-16 SSL Communication



## Configuring MWTM with IOS Server Load Balancing

If a network failure causes the MWTM software to fail, you can no longer monitor your network. You can solve this potential problem by configuring a backup MWTM server, as detailed in [Configuring a Backup MWTM Server, page 3-10](#). However, this solution requires a connection to the backup MWTM server, which might not mirror exactly the primary MWTM server.

A better solution is to use IOS Server Load Balancing (IOS SLB), which provides transparent failover of the MWTM client connection.

Use this procedure to configure the MWTM software with IOS SLB:

**Step 1** Ensure that you have this required hardware and software:

- Solaris/Linux server with at least two network interface cards (NICs)
- Cisco 7204VXR or 7206VXR series node
- IOS SLB release 12.1(11b)E or later
- MWTM release 6.1 or later

- Step 2** Configure the Solaris/Linux server with at least two active NICs.
- Step 3** Configure a routing protocol on the Solaris/Linux server, such that if one network interface fails, the other interfaces can still contact the monitored networks and the MWTM client:
- Run **in.routed** on the Solaris/Linux server, with two RIP-based nodes on two separate networks providing routing tables for the server. See the **in.routed** man page for more information on this configuration.
  - Use the GateD routing software developed by NextHop Technologies.
- Step 4** Configure the Cisco 7204VXR or 7206VXR series router, with the Solaris/Linux server network interfaces configured as real servers in the server farm. Refer to the IOS SLB feature module for more information on configuring the IOS SLB node.
- Step 5** Configure a virtual interface, lo0:1 with the Internet address that matches the virtual IP address configured on the IOS SLB node:
- ```
ifconfig lo0:1 addif ip-address
```
- Step 6** Install the MWTM software.
- Step 7** Edit the */opt/CSCOs/gm/properties/System.properties* file, and replace the SERVER NAME variable with the DNS entry that matches the virtual IP address configured on the IOS SLB node. Save your changes and restart the MWTM server.
- Step 8** Configure your MWTM clients to match the same DNS entry.
- Step 9** Your configuration is complete.
-

Remember that:

- Failover of the MWTM client is transparent to the user. No additional changes are needed at that end.
- A failure of either interface, or of the surrounding networks, might cause the MWTM client to hang for a short period, depending on the convergence of the routing protocol used by the MWTM server. For example, with RIP, the MWTM client might hang for up to two minutes while RIP converges after a network failure. Faster protocols might result in shorter MWTM client hang times.



MWTM Ports

The Cisco Mobile Wireless Transport Manager (MWTM) uses the following default ports to provide services:

Port Name or Number	Port Type	Description
1774	tcp	Apache web server
1775	tcp	TOMCAT Java Server Pages (JSP) server
44742	tcp	Java Remote Method Invocation (RMI) naming service
dynamic port 1	tcp	Java RMI service for Login Service. A network or system administrator can specify a fixed port using the LOGINSERVER_PORT parameter in the <i>System.properties</i> file. Note If you installed the MWTM in the default directory, <i>/opt</i>, then the location of the <i>System.properties</i> file is <i>/opt/CSCOsgm/properties/System.properties</i>. If you installed the MWTM in a different directory, then the <i>System.properties</i> file resides in that directory.
dynamic port 2	tcp	Java RMI service for the MWTM Data Server. A network or system administrator can specify a fixed port using the DATASERVER_PORT parameter in the <i>System.properties</i> file. Note If you installed the MWTM in the default directory, <i>/opt</i>, then the location of the <i>System.properties</i> file is <i>/opt/CSCOsgm/properties/System.properties</i>. If you installed the MWTM in a different directory, then the <i>System.properties</i> file resides in that directory.

Port Name or Number	Port Type	Description
162	udp	Simple Network Management Protocol (SNMP) trap listener
dynamic ports 1-25	udp	SNMP request senders. These ports are used by the SNMP stack for sending SNMP requests. A maximum of 25 can be opened in the MWTM. You can customize the number of ports by changing the <code>SNMP_SOCKET_NUMBER</code> parameter in the <i>Server.properties</i> file. Note If you installed the MWTM in the default directory, <i>/opt</i>, then the location of the <i>Server.properties</i> file is <i>/opt/CSCOsgm/properties/Server.properties</i>. If you installed the MWTM in a different directory, then the <i>Server.properties</i> file resides in that directory.



GLOSSARY

This glossary contains Cisco Mobile Wireless Transport Manager (MWTM) specific terms. For an online listing of other internetworking terms and acronyms, refer to this URL:

http://www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html

A

access list	A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
accounting	Collection of SS7 accounting statistics.
adjacent node	In the MWTM, for a given pair of connected nodes, the node that the MWTM discovered second. See primary node .
adjacent point code	Point code of the adjacent ITP signaling point for the linkset. Contrast with local point code .
aggregation site	A Base Station Controller (BSC) or Radio Network Controller (RNC) site where traffic is collected for multiple cell sites. See cell site .
alarm	An alarm is a sequence of events, each representing a specific occurrence in the alarm lifecycle. The lifecycle of an alarm can include any number of related events that are triggered by changes in severity, updates to services, and so on. See event .
alias point code	See capability point code .
ANSI	American National Standards Institute.
API	Application Programming Interface. A source code interface that a computer system or program library provides to support requests for services by a computer program.
application server	Logical entity serving a specific routing key. The application server implements a set of one or more unique application server processes, of which one or more is normally actively processing traffic. See application server process , application server process association , routing key , signaling gateway-mated pair .
application server process	IP-based instance of an application server, such as Call Agents, HLRs, SMSCs, and so on. An application server process can implement more than one application server. See application server , application server process association , routing key , signaling gateway-mated pair .
application server process association	ITP's virtual view of an application server process. The application server process association is defined on, and resides on, the ITP. See application server , application server process , routing key , signaling gateway-mated pair .
arrowhead	In topology maps, indicator for an application server process association connection. See topology map .

- auto save** Setting that enables the MWTM to save changes automatically when you exit the MWTM.
- auto start** Setting that enables the MWTM to start a process automatically when the Process Manager is started. See [Data Server](#), [Message Log Server](#), [Process Manager](#), [Trap Receiver](#).

B

- base station controller** See [BSC](#).
- base transceiver station** See [BTS](#).
- browser** GUI-based hypertext client application, such as Internet Explorer or Mozilla, used to access hypertext documents and other services located on innumerable remote servers throughout the World Wide Web (WWW) and Internet.
- BSC** Base Station Controller. Equipment that manages radio resources in a GSM network.
- BTS** Base Transceiver Station. The equipment in a GSM network that is used to transmit radio frequencies over the air waves.

C

- capability point code** Point code shared by more than one signaling point, each of which is also assigned a “real” point code. Also called [alias point code](#).
- cell site** A Base Transceiver Station (BTS) or Node B site, usually located at the remote site with limited connectivity. See [aggregation site](#).
- circle** In topology maps, indicator for a link that is part of a virtual linkset, associated with the closest node. See [topology](#).
- circle layout** Topology map layout in which objects are arranged in a circle, connected by links. Contrast with [spring layout](#). See [topology map](#).
- Cisco IOS software** Cisco Internetwork Operating System software. Cisco system software that provides common functionality, scalability, and security for many Cisco products. The Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms.
- CLI** Command line interface. An interface that allows the user to interact with the Cisco IOS software operating system by entering commands and optional arguments.
- client** Node or software program that requests services from a server. The MWTM user interface is an example of a client. See also [server](#).
- client view** User-customized subset of the DEFAULT view. See also [DEFAULT view](#), [view](#), [subview](#).
- CLLI code** COMMON LANGUAGE Location Identification Code for a node. A CLLI code is a standardized 11-character identifier that uniquely identifies the geographic location of the node.

command line interface	See CLI .
community name	See community string .
community string	Text string that acts as a password and is used to authenticate messages sent between a management station and a node containing an SNMP agent. The community string is sent in every packet between the manager and the agent. Also called community name , read community .
congestion	Condition in which a link has too many packets waiting to be sent. This condition could be caused by the failure of an element in the network. Possible levels are None, Low, High, and Very High, which correspond roughly to equivalent ANSI, China standard, ITU, NTT, and TTC congestion levels.
console log	Log containing unexpected error and warning messages from the MWTM server, such as those that might occur if the MWTM server cannot start.
cost	Measure of the suitability of a route to a destination, relative to other routes. Costs range from 1 (lowest cost and highest priority) through 9 (highest cost and lowest priority).
credentials	Login credentials that are stored in an encrypted file on the server, eliminating the need for users to login before running commands. The MWTM enables a system administrator to configure the login credentials using the Node SNMP and Credentials Editor dialog box.
cross-instance GTT file	Global Title Translation file that supports the Multiple Instance and Instance Translation ITP features. Cross-instance GTT files contain application groups that reference point codes in other GTT files. See Instance Translation , Multiple Instance .
CSV	Comma-separated values. A widely-used file format for storing tabular data.
current view	View that is currently in use on an MWTM client. The view can be the DEFAULT view or a customized view. Also called current view . See client view , DEFAULT view .
D	
Data Server	Multi-threaded process that handles most of the work done by the MWTM, including discovery, polling, and scheduling. See also Message Log Server , Process Manager , Trap Receiver .
DEFAULT view	View into which the MWTM places all discovered objects when discovering the network. The DEFAULT view is stored on the MWTM server and shared by all MWTM clients, but it cannot be modified by the clients. See current view , view .
demand polling	User-initiated poll of selected nodes. Contrast with status polling .
destination linkset	In ITP route tables, linkset associated with the destination point code. Also called the output linkset . See linkset , destination point code , route table .
destination point code	In ITP route tables, point code of the adjacent signaling point, the destination for packets on the selected signaling point. See destination linkset , point code , route table .
device	See node .
device type	In MWTM, the type of a discovered device, either a Cisco device or a BTS, BSC, or legacy SS7 device. Also called system object ID . See legacy device .

diamond	In topology maps, indicator for a connection that is part of a configured interface, associated with the closest node. See topology .
discovered	Object that has been discovered by the MWTM. Also called <i>known</i> . Contrast with unknown .
Discovery	Process by which the MWTM discovers objects in your network. See also nonrecursive Discovery , recursive Discovery .
display name	User-specified name for a node. Contrast with DNS name . See also node name .
domain name	The style of identifier—a sequence of case-insensitive ASCII labels separated by dots (“bbn.com.”)—defined for subtrees in the Internet Domain Name System [R1034] and used in other Internet identifiers, such as host names, mailbox names, and URLs.
Domain Name System	See DNS .
double triangle	In topology maps, indicator for a connection that has multiple interfaces, such as two linksets between the same two signaling points. See topology map .
DNS	Domain Name System. System used on the Internet for translating names of network nodes into addresses.
DNS name	Initial name of a node, as discovered by the MWTM. Contrast with display name . See also node name .
DPC	See destination point code .

E

Erlang (E)	The international (dimensionless) unit of the average traffic intensity (occupancy) of a facility during a period of time, normally, a busy hour. The number of Erlangs is the ratio of the time during which a facility is occupied (continuously or cumulatively) to the time this facility is available for occupancy. Another definition is the ratio of the average call arrival rate into the system, to the average call duration. One Erlang is equivalent to 36 ccs (completed call seconds), which is another traffic intensity unit.
event	An event is a singular occurrence in time. Events are derived from incoming traps and notifications, and from detected status changes. The MWTM can detect events that are triggered by SNMP traps or notifications, status changes, and user actions. See trap, alarm.
event forwarding	See trap forwarding .
exclude	Removing a network object from a view, while retaining the object in the MWTM database.

F

Field Replaceable Units See [FRU](#).

FRU Assemblies such as power supplies, fans, processor modules, interface modules, and so forth.

G

GGSN Gateway GPRS Support Node. A gateway that provides mobile cell phone users access to a public data network or specified private IP networks.

GPRS General Packet Radio Service. A 2.5G mobile communications technology that enables mobile wireless service providers to offer their mobile subscribers packet-based data services over GSM networks.

GSM ITU standard for defining the Global System for Mobile communications, a digital cellular telephone standard.

Global System for Mobile communications See [GSM](#).

graphical element Graphical representation of an object or view in the topology map. See [topology map](#).

graphical user interface See [GUI](#).

GTP GPRS Tunneling Protocol. A protocol that enables the connection between the SGSN and the GGSN.

GTT Global Title Translation. The process by which the SCCP translates a global title into the point code and subsystem number of the destination service switching point where the higher-layer protocol processing occurs.

GUI Graphical user interface. User environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored. Conventions such as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms utilizing a GUI.

H

host Computer system on a network. Similar to the term node except that host usually implies a computer system, whereas node generally applies to any network system, including access servers and ITP, IPRAN, or mSEF devices. See also [node](#).

host address See [host number](#).

host number Part of an IP address that designates which node on the subnetwork is being addressed. Also called a [host address](#).

HSL	High-speed link. An HSL link is one that uses the SS7-over-ATM (Asynchronous Transfer Mode) high-speed protocol.
HTML	Hypertext Markup Language. Simple hypertext document formatting language that uses tags to indicate how a given part of a document should be interpreted by a viewing application, such as a web browser. See also hypertext and browser .
hypertext	Electronically-stored text that allows direct access to other texts by way of encoded links. Hypertext documents can be created using HTML, and often integrate images, sound, and other media that are commonly viewed using a browser. See also HTML and browser .
Hypertext Markup Language	See HTML .
I	
ignore	Exclude an object when aggregating and displaying MWTM status information. See also unignore .
IMSI	International Mobile Subscriber Identity. A unique 15-digit code that identifies an individual user on a GSM network.
installation log	Log containing messages and other information recorded during installation.
Instance Translation	ITP feature in support of the Multiple Instance feature that enables the conversion of packets between instances of any variant. Each instance is a separate domain with a defined variant, network indicator, ITP point code, optional capability point code, and optional secondary point code. Each instance also has its own routing table and GTT file. See cross-instance GTT file , Multiple Instance .
interface	Connection between two systems or devices. In the MWTM, an interface is a connection on an ITP, IPRAN, or mSEF node.
internal ID	Unique identifier assigned by the MWTM, for its own internal use, to every event, link, linkset, and node.
Internet Protocol	See IP .
IP	Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Documented in RFC 791.
IP address	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. See also IP .
IP backhaul	A trunk that transports optimized voice and data traffic between a remote cell-site, RAN-O node and an aggregation RAN-O node at a central site.

ITP	Part of Cisco's hardware and software SS7-over-IP (SS7oIP) solution. ITP provides a reliable, cost-effective medium for migrating Signaling System 7 (SS7), the telecommunications network signaling technology, to the mobile wireless industry IP environment. ITP off-loads SS7 Short Messaging Service (SMS) traffic onto the IP network, replacing the mobile service provider's signaling network with a redundant IP cloud.
ITU	International Telecommunication Union.
K	
known	See discovered .
L	
LAN	Local Area Network.
legacy device	In the MWTM, an SS7 device that is not a Cisco ITP or a Cisco RAN-O node. Legacy devices include MSCs, SCPs, SSPs, STPs, BSCs, and BTSs. See MSC , SCP , SS7 , SSP , STP , BTS , BSC .
link	In ITP, the connection between nodes. See ITP , linkset , node .
link type	In the MWTM, the type of a discovered ITP link, either SCTP IP or serial. See HSL , SCTP , serial , virtual link .
linkset	In ITP, a grouped set of links. In the MWTM, a representation of two linksets associated with two nodes, one for each side of a logical connection. See ITP , link , node .
linkset pair	In the MWTM, a single linkset with input from the perspective of both of its endpoints. See also linkset .
linkset type	In the MWTM, the type of a discovered linkset, either SCTP IP, serial, HSL, mixed, or other. Other means no links have been defined for the linkset. See HSL , mixed linkset , SCTP , serial , virtual linkset .
local authentication	Type of MWTM security authentication that allows the creation of user accounts and passwords local to the MWTM system. When using this method, user names, passwords, and access levels are managed using MWTM commands. Contrast with Solaris authentication . For more information on Solaris authentication, see the "Implementing Secure User Access (Server Only)" section on page 2.
local IP address	IP address used by the MWTM client to connect to the MWTM server.
local point code	Point code of the primary signaling point for a linkset. Contrast with adjacent point code .
local VPN IP address	IP address used by the MWTM client to connect to the MWTM server via VPN. See local IP address , VPN .

M

M3UA	MTP3 User Adaptation layer. A protocol for supporting the transport of any SS7 MTP3 user signaling over the IP network. M3UA provides a seamless operation of the MTP3 user peers in the SS7 and IP domains. See MTP3 .
managed object	Node, application server, application server process, application server process association, link, linkset, node, signaling gateway-mated pair, or signaling point that is being managed by the MWTM.
Management Information Base	See MIB .
MAP	Mobile Application Part. An SS7 protocol that allows for the implementation of mobile network signaling infrastructure. See SS7 .
mask	Bit combination used in the MWTM to indicate the significant bits of the point code. For ANSI and China standard networks using the default 24-bit point code format, the default mask is 255.255.255. For ITU networks using the default 14-bit point code format, the default mask is 7.255.7. For NTT and TTC networks using the default 16-bit point code format, the default mask is 31.15.127.
Message Log Server	Multi-threaded process that logs messages from the Data Server, Process Manager, and MWTM client. See also Data Server , Process Manager , Trap Receiver .
MIB	Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
mixed linkset	Linkset in which the links are of two or more types. (This configuration is not recommended.)
MLR	Multi-Layer SMS Routing. Scheme that enables intelligent routing of Short Message Service (SMS) mobile originated (MO) messages based on the application or service from which they originated or to which they are destined. The MLR feature can make SMS message routing decisions based on information found in the TCAP, MAP, and MAP-user layers; MAP operation codes MAP-MT-FORWARD-SM and SEND-ROUTING-INFO-FOR-SM; and ANSI TCAP and IS-41 MAP operations.
mobile switching center	See MSC .
MSC	Mobile switching center. Provides telephony switching services and controls calls between telephone and data systems.
MSU	Message Signal Unit. MSUs provide MTP protocol fields and are the workhorses of the SS7 network. All signaling associated with call setup and teardown, database query and response, and SS7 management requires the use of MSUs. See MTP3 .

MTP3	Message Transfer Part, level 3. An SS7 protocol that routes SS7 signaling messages to public network nodes by means of destination point codes, which allow messages to be addressed to specific signaling points. See SS7 .
Multi-Layer SMS Routing	See MLR .
Multiple Instance	ITP feature that makes it possible to connect an ITP to different networks at one time, each with specific variant and network indicator values. The ITP treats each combination of variant and network indicator as a separate “instance” or signaling point with its own local point code and routing table on the ITP. Each instance is part of the SS7 network and shares the same variant and network indicator. In order for instances in the same network to be properly managed they must be assigned the same network name. See cross-instance GTT file , Instance Translation .
N	
name server	Server connected to a network that resolves network names into network addresses.
NAT	Network Address Translation. Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.
Network Address Translation	See NAT .
network indicator	See NI .
network management system	See NMS .
network view	See view .
Network Time Protocol	See NTP .
new node	Node that the MWTM has newly discovered, and that has not yet been added to the current view.
NI	Network indicator. Information within the service information octet of the MSU that permits discrimination between national and international messages. See MSU .
NMS	Network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer such as an engineering workstation. NMSes communicate with agents to help keep track of network statistics and resources.

node Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations. Nodes, which vary in routing and other functional capabilities, can be interconnected by links, and serve as control points in the network.

In ITP, a node is a Cisco ITP or a legacy SS7 device (SSP, SCP, or STP).

In RAN-O networks, a node is a Cisco Mobile Wireless Router (MWR), Optical Networking System (ONS), RAN service module, or a legacy RAN device (BTS or BSC).

See [legacy device](#).

Node B Physical unit for radio transmission/reception with cells in the UTRAN.

node name Name of a node. This is either the DNS name of the node, or a user-specified name. See [display name](#), [DNS name](#).

nonrecursive Discovery Discovery of seed nodes only. The MWTM discovers all seed nodes and attempts to manage them, then marks all nodes that are adjacent to those seed nodes as Unmanaged. Contrast with [recursive Discovery](#).

Non-Stop Operation See [NSO](#).

note User-defined descriptive string attached to an object.

NSO Non-Stop Operation. Implementation of redundant data elements and software functionality, enabling networks to approach 99.999% availability. See also [RF](#).

NTP Network Time Protocol. Timing protocol that maintains a common time among Internet hosts in a network.

O

object Node, application server, application server process, application server process association, link, linkset, node, signaling gateway-mated pair, or signaling point that has been discovered by the MWTM.

output linkset See [destination linkset](#).

P

PDP Packet Data Protocol. Network protocol used by external packet data networks that communicate with a GPRS network. IP is an example of a PDP supported by GPRS. Refers to a set of information (such as a charging ID) that describes a mobile wireless service call or session, which is used by mobile stations and GGSNs in a GPRS network to identify the session.

PDU Protocol Data Unit. OSI term for packet.

ping Packet internet groper. ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

point code	A unique address code that identifies a service provider within a signaling network. Also called primary point code . See capability point code , destination point code , local point code , secondary point code .
polling	Access method in which a primary network device inquires, in an orderly fashion, whether secondaries have data to transmit. The inquiry occurs in the form of a message to each secondary that gives the secondary the right to transmit.
poll interval	Time between polls.
poll response	Time taken by a node to respond to MWTM poll requests.
port	In IP terminology, an upper-layer process that receives information from lower layers. Ports are numbered, and each numbered port is associated with a specific process. For example, SMTP is associated with port 25. A port number is also called a well-known address.
preferences	Settings that enable a user to change the way the MWTM presents information.
primary node	In the MWTM, for a given pair of connected signaling points or nodes, the signaling point or node that the MWTM discovered first. See adjacent node .
primary point code	See point code .
primary SNMP address	IP address used by SNMP to poll the node. (There might be other IP addresses on the node that are not the primary SNMP address.) Contrast with secondary IP address .
process	Internal component of the MWTM. See Data Server , Message Log Server , Process Manager , Trap Receiver .
Process Manager	Multi-threaded process that handles the management of registered MWTM processes. See also Data Server , Message Log Server , Trap Receiver .
Q	
QoS	Quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
Quality of Service	See QoS .
R	
Radio Network Controller	See RNC .
RAN	Radio Access Network.
RAN backhaul	The end-to-end RAN connections between the BTS or Node B at the cell site and the BSC or RNC. See also virtual RAN backhaul , IP backhaul .

RAN shorthaul	An interface that transports GSM or UMTS voice and data traffic between the BTS or Node-B and the RAN-O node at the cell site. At the aggregation site, RAN shorthauls exist between the RAN-O node and the BSC or RNC.
RAN-O	RAN optimization. Standard-based, end-to-end, IP connectivity for GSM and UMTS RAN transport. The Cisco solution puts RAN voice and data frames into IP packets at the cell-site, and transports them seamlessly over an optimized backhaul network. At the central site, the RAN frames are extracted from IP packets, and the GSM or UMTS data streams are rebuilt.
read community	See community string .
recursive Discovery	Discovery of the entire network. The MWTM discovers all seed nodes and attempts to manage them; then attempts to discover and manage all ITP nodes that are adjacent to those seed nodes (unless the nodes are connected by serial links only); then attempts to discover and manage all ITP nodes that are adjacent to <i>those</i> nodes; and so on, until the MWTM has discovered the entire network. Contrast with nonrecursive Discovery .
Redundancy Framework	See RF .
RF	Redundancy Framework. Mechanism for logical redundancy of software functionality, designed to support 1:1 redundancy on processor cards. See also NSO .
RNC	Radio Network Controller. Network element that controls one or more Node B transceiver stations in the UTRAN.
route	Path through an internetwork.
route set	Set of routes with the same destination point code.
route table	Table used in ITP to locate a destination linkset for a packet whose destination point code does not match the ITP's local point code.
routing key	Set of SS7 parameters that uniquely define the range of signaling traffic to be handled by a particular application server or application server route table. Thus, the routing key identifies an application server or an application server route table. See application server , application server process , application server process association , signaling gateway-mated pair

S

SCCP	Signaling Connection Control Part. A routing protocol in SS7 protocol suite in layer 4 that provides end-to-end routing for TCAP messages. SCCP also provides the means by which an STP can perform global title translation, a procedure by which the destination signaling point and subsystem number is determined from digits present in the signaling message. See also TCAP .
SCP	Service control point. An element of an SS7-based Intelligent Network that performs various service functions, such as number translation, call setup and teardown, and so on.
SCTP	Stream Control Transmission Protocol. An end-to-end, connection-oriented protocol that transports data in independent sequenced streams.

secondary IP address	Alternate or backup IP address used by a node. Contrast with primary SNMP address .
secondary point code	Alternate or backup point code used by a signaling point. See point code .
seed file	List of seed nodes. See seed node .
seed node	Node used by the MWTM to discover the other objects in your network.
serial	Method of data transmission in which the bits of a data character are transmitted sequentially over a single channel.
server	Node or software program that provides services to clients. See client .
service control point	See SCP .
service switching point	See SSP .
SGMP	See signaling gateway-mated pair .
SGSN	Serving GPRS Support Node. Node that connects the radio access network to the GPRS or UMTS core and tunnels user sessions to the GGSN.
signaling gateway-mated pair	Pair of signaling gateways that exchange necessary state information using the Signaling Gateway-Mated Protocol (SGMP). See application server , application server process , application server process association , routing key , signaling gateway-mated pair .
Signaling Gateway-Mated Protocol	Protocol that enables two Cisco ITP M3UA/SUA signaling gateways to act as a mated pair and exchange necessary state information. See signaling gateway-mated pair .
signaling point	See SP .
signal transfer point	See STP .
Signaling System 7	See SS7 .
Simple Network Management Protocol	See SNMP .
SMPP	Short Message Peer-to-Peer Protocol. A messaging protocol meant to simplify integration of data applications with wireless mobile networks such as GSM.
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SOAP	Simple Object Access Protocol. A protocol for exchanging XML-based messages over computer networks. See XML .

Solaris authentication	Type of MWTM security authentication that uses standard Solaris-based user accounts and passwords, as specified in the <i>/etc/nsswitch.conf</i> file. You can provide authentication with the local <i>/etc/passwd</i> file or from a distributed Network Information Services (NIS) system. Contrast with local authentication. For more information on Solaris authentication, see the “Implementing Secure User Access (Server Only)” section on page 2.
SP	Signaling point. An SCP, SSP, or STP, or an ITP instance. See SCP, SSP, or STP.
spring layout	Topology map layout in which objects are arranged in a spring layout. Objects with the most links are drawn closer to the center of the map, while objects with fewer links are drawn farther away. Contrast with circle layout. See topology map.
SS7	Signaling System 7. Standard CCS system used with BISDN and ISDN. Developed by Bellcore.
SSL	Secure Sockets Layer. A protocol for transmitting private documents via the Internet.
SSP	Service switching point. Element of an SS7-based Intelligent Network that performs call origination, termination, or tandem switching.
status	Current condition, such as Active or Unknown, of a network object.
status polling	Regularly scheduled polling of nodes performed by the MWTM. Contrast with demand polling.
STP	Signal transfer point. Element of an SS7-based Intelligent Network that performs routing of the SS7 signaling.
SUA	SCCP User Adaptation. A client/server protocol that provides a gateway to the legacy SS7 network for IP-based applications that interface at the SCCP layer. See also SCCP.
Stream Control Transmission Protocol	See SCTP.
subview	A view within a customized view. You can create subviews on an MWTM client, with each subview devoted to a different part of the network. You can then load a subview to manage a different part of the network, or switch to the DEFAULT view to see the entire network. See also DEFAULT view.
superuser	User specified in the MWTM to be able to perform most functions that otherwise require the user to be logged in as the root user. For more information, see the “Specifying a Super User (Server Only)” section on page 20.
system object ID	See device type.

T

TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. See also TCP/IP.
TCAP	Transaction Capabilities Application Part. An SS7 protocol that enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the SCCP connectionless service. See also SCCP.

TCP/IP	Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite. See also IP and TCP .
TFTP	Trivial File Transfer Protocol. A protocol that is used to transfer small files between hosts of a network. See also host .
thread name	Task name.
timeout	Event that occurs when one network device expects to hear from another network device within a specified period of time, but does not. The resulting timeout usually results in a retransmission of information or the dissolving of the session between the two devices.
tooltip	Popups that display information about objects and table entries.
topology	See topology map .
topology map	Graphical representation by the MWTM of the network. Also called topology .
Transmission Control Protocol	See TCP .
Transmission Control Protocol/Internet Protocol	See TCP/IP .
trap	Unsolicited message sent by an SNMP agent to an NMS, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that has been reached.
trap forwarding	Forwarding MWTM events to other hosts, in the form of SNMP traps. This enables the MWTM to integrate with high-level event- and alarm-monitoring systems such as the Cisco Info Center (CIC) and Micromuse's Netcool suite of products. These systems can provide a single high-level view of all alarm monitoring in your network, making it easier to detect and resolve problems.
Trap Receiver	Multi-threaded process that receives SNMP traps for the MWTM. See also Data Server , Message Log Server , Process Manager .
Trivial File Transfer Protocol	See TFTP .
U	
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
UMTS	Universal Mobile Telecommunications System. Third generation wireless standard for supporting data transfer rates of 144 kbs (vehicular), 384 kbs (pedestrian), or up to 2 Mbps in buildings.
UMTS Terrestrial RAN	See UTRAN .

unignore	Stop ignoring the selected object at the next polling cycle. See also ignore .
unknown	Device type for which the MWTM is unable to determine the device type. If a node, the node failed to respond to an SNMP request. If a linkset or link, either the associated node failed to respond to an SNMP request, or the MWTM found that the linkset or link no longer exists. Contrast with discovered .
Universal Mobile Telecommunications System	See UMTS .
unmanaged	Node status in which the node is known indirectly by the MWTM (the MWTM knows the device exists but no known SNMP stack exists on the device for the MWTM to query), or a user has set the node to this status to prevent the MWTM from polling the node.
User-Based Access	MWTM security scheme that provides multi-level password-protected access to MWTM features. Each user can have a unique user name and password. Each user can also be assigned to one of five levels of access, which control the list of MWTM features accessible by that user. For more information, see the “Configuring User Access” section in Chapter 2, “Configuring Security.”
User Datagram Protocol	See UDP .
utilization	Amount of an object’s send or receive capacity that is being used, expressed as a percentage or in Erlangs.
UTRAN	UMTS Terrestrial RAN. Radio access network for UMTS networks.
V	
variant	A method of identifying SS7 point codes. Example point code variants are: ITU: 3-8-3 format is common, made up of 14 bits ANSI: 8-8-8 format is common, made up of 24 bits
view	View that is currently in use on an MWTM client. The current view can be the DEFAULT view or a customized view. A customized view can have one or more subviews. See client view , current view , DEFAULT view .
virtual RAN backhaul	A grouping of RAN backhauls. A virtual RAN backhaul is useful if you have configured several RAN backhauls for the same interface. To view the utilization for that interface, create a virtual RAN backhaul that contains all the real backhauls that you have configured for the interface. See RAN backhaul .
virtual link	Link that connects signaling point instances running on the same device. The MWTM does not poll virtual links, nor does it display real-time data or accounting statistics for virtual links.

virtual linkset

Linkset in which the links are virtual links, which connect signaling point instances running on the same device. The MWTM does not poll virtual linksets, nor does it display real-time data or accounting statistics for virtual linksets.

**Note**

Prior to IOS release 12.2(23)SW1, virtual linksets on multi-instance routers were created manually by the user. Within and after that release, virtual linksets are created automatically.

Virtual Private Network

See [VPN](#).

VPN

Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

W**World Wide Web**

See [WWW](#).

WWW

World Wide Web. Large network of Internet servers providing hypertext and other services to terminals running client applications such as a browser. See also *browser*.

X**XML**

Extended Markup Language. A general-purpose markup language for to facilitating the sharing of data across different information systems connected through the Internet. See [SOAP](#).



INDEX

A

- access
 - node [4-4](#)
- accessing
 - MWTM web browser [4-28](#)
- accounting
 - FAQs [C-14](#)
- address
 - information [8-14](#)
- address tables [15-1](#)
 - editor
 - launching [15-2](#)
 - startup options [15-2](#)
 - files
 - basic information [15-19](#)
 - creating [15-6](#)
 - deploying [15-18](#)
 - loading, from file [15-8](#)
 - loading, from ITP [15-10](#)
 - reverting [15-25](#)
 - saving [15-23](#)
 - semantics [15-17](#)
 - working [15-14](#)
 - listing [15-20](#)
 - menu [15-3](#)
 - properties
 - editing [15-17](#)
- administrative page
 - displaying [11-12](#)
- alarm
 - filter
 - loading [9-25](#)
 - setting [9-18](#)
- alarm filter
 - dialog
 - buttons [9-19](#)
 - loading [9-25](#)
 - saving [9-26](#)
 - setting [9-18](#)
- alarms
 - displaying [9-8, 11-30](#)
 - right-click menu [9-16](#)
 - viewing [8-45](#)
- application server
 - reports [12-9](#)
 - tabs [A-9](#)
- application server process
 - tabs [A-10](#)
- application server process association
 - configuration
 - general information [8-16](#)
 - tabs [A-10](#)
- application server process associations
 - status definitions [E-4](#)
 - table [6-18](#)
- application server processes
 - export files, daily [12-51](#)
 - reports
 - daily [12-13, 12-14](#)
 - hourly [12-12](#)
 - peaks [12-15, 12-16](#)
 - status definitions [E-4](#)
 - table [6-16](#)
- application servers
 - configuration

- associations [8-14](#)
- export files, hourly [12-51](#)
- reports
 - daily [12-10, 12-50](#)
 - hourly [12-50](#)
 - peaks [12-11](#)
- statistics details window [8-66](#)
- status definitions [E-4](#)
- table [6-14](#)

AS

- custom reports, accounting [12-57](#)
- export files, daily [12-44](#)
- reports
 - custom [12-57](#)

AS accounting

- reports [12-44](#)

ASP accounting

- reports [12-44](#)

asterisks

- FAQs [C-14](#)

attaching

- notes [6-38](#)

audience

- document [iii-xxxii](#)

B

- backup
 - MWTM files [2-32](#)
 - secondary server [3-10](#)
- basic object functions
 - understanding [6-1](#)
- browser
 - FAQs [C-6](#)
- BWG
 - traps [G-18](#)

C

- capacity planning
 - FAQs [C-20](#)
- card
 - naming
 - information [8-22](#)
 - table [6-23](#)
 - tabs [A-12](#)
- changing
 - client preference, settings [5-1](#)
 - poller settings [3-2](#)
 - web preference, settings [5-1](#)
- charts
 - settings
 - changing [5-11](#)
- CiscoWorks
 - integrating with MWTM [5-39](#)
 - SNMP [3-2](#)
- client, MWTM
 - access, limiting [2-31](#)
 - downloading (see MWTM web interface)
 - exiting [4-32](#)
 - launching from Windows Start menu [4-31](#)
 - starting
 - on Solaris/Linux [4-3](#)
 - on Windows [4-4](#)
 - prerequisites [4-3](#)
- client/server architecture, overview [1-10](#)
- client A configuration
 - MWTM [H-16](#)
- client B configuration
 - MWTM [H-16](#)
- client preference, settings
 - changing [5-1](#)
- clients, MWTM
 - connection timer [3-11](#)
- color
 - severity

- customizing [5-18](#)
- command
 - reference [B-1](#)
- command line interface, using [5-47](#)
- commands
 - general [B-1](#)
 - ITP [B-85](#)
- configuration
 - sample firewall [H-10](#)
- configuring
 - firewalls [H-8](#)
 - port numbers and parameters [H-7](#)
- connection settings [5-7](#)
- connection timer [3-11](#)
- content area
 - MWTM client [4-19](#)
- conventions
 - document [iii-xxxiii](#)
- conversion entry
 - table [14-14](#)
- counters
 - resetting [5-21](#)
- CPU
 - performance, viewing [8-58](#)
- credentials, login
 - setting up [3-20](#)
- CSG
 - MIBS
 - specific [F-5, F-6](#)
- CSG1
 - traps [G-14](#)
- CSG2
 - traps [G-15](#)
- customizing view [7-9](#)
- custom reports
 - AS, accounting [12-57](#)
 - generating [12-3](#)
 - MTP3, accounting [12-57](#)

D

- data
 - accessing, from web [11-1](#)
 - exporting [5-38](#)
 - MWTM
 - exporting current, for node names [5-39](#)
 - exporting current, for SNMP community names [5-39](#)
- data, removing from server [2-35](#)
- default
 - server name, changing [4-31](#)
 - view
 - loading [7-14](#)
- deleting
 - objects [6-40](#)
- deploying
 - GTT [14-37](#)
- deployment
 - FAQs [C-14](#)
- details
 - viewing [8-12](#)
- device configuration
 - buttons [3-22](#)
 - commands [3-23](#)
 - menu [3-15](#)
- device configuration dialog [3-14](#)
- diagram, network [10-1](#)
- discovering ITP networks
 - dialog menu [4-6](#)
 - discovered nodes [4-15](#)
 - running discovery [4-12](#)
 - settings [4-13](#)
 - verifying discovery [4-15](#)
- discovery
 - FAQs [C-13](#)
- display, customizing [7-9](#)
- displaying [11-31](#)
 - administrative page [11-12](#)

- alarms [9-8, 11-30](#)
 - error statistics [11-39](#)
 - events [9-8, 11-30](#)
 - objects within a view [11-33](#)
 - performance statistics [11-34](#)
 - RAN data export files [11-43](#)
 - reports [11-33](#)
 - software versions [11-31](#)
 - DISPLAY variable, setting [4-3](#)
 - document
 - audience [iii-xxxii](#)
 - conventions [iii-xxxiii](#)
 - objectives [iii-xxxi](#)
 - organization [iii-xxxii](#)
 - documentation
 - related [iii-xxxiv](#)
 - DOS prompt, launching [4-31](#)
 - dual-interface machine
 - MWTM, configuring [H-14](#)
-
- ## E
- editing
 - MWTM
 - ITP route table file [13-1](#)
 - properties [6-33](#)
 - error data
 - viewing [8-115](#)
 - error statistics
 - displaying [11-39](#)
 - event
 - adding sound files [9-52](#)
 - attaching notes [9-29](#)
 - categories [9-41](#)
 - filter
 - loading [9-25](#)
 - setting [9-18](#)
 - forwarding as traps [9-48](#)
 - limits [9-37](#)
 - managing [9-1](#)
 - playing or muting sounds [9-53](#)
 - properties
 - viewing [9-27](#)
 - settings
 - categories [5-9](#)
 - changing [5-8](#)
 - colors [5-8](#)
 - date [5-9](#)
 - time [5-9](#)
 - SNMP servers and traps [9-40](#)
 - sound filters
 - creating new [9-50](#)
 - deleting [9-53](#)
 - listing [9-49](#)
 - sounds, setting [9-49](#)
 - traps [9-42](#)
 - event editor [9-35](#)
 - categories [9-41](#)
 - launching [4-31](#)
 - limits [9-37](#)
 - SNMP servers and traps [9-40](#)
 - traps [9-42](#)
 - event files
 - archived
 - viewing [9-30](#)
 - event filter
 - dialog
 - buttons [9-19](#)
 - properties [9-19](#)
 - selected objects [9-21](#)
 - example [9-25](#)
 - loading [9-25](#)
 - saving [9-26](#)
 - setting [9-18](#)
 - events
 - displaying [9-8, 11-30](#)
 - settings
 - other [5-11](#)

- severities [5-10](#)
- sound filters
 - changing [9-53](#)
- window
 - toolbar buttons [9-14](#)
- events and alarms
 - FAQs [C-7](#)
- excluding
 - objects
 - ITP reports [12-4](#)
- exit
 - settings [5-4](#)
- export files
 - application server processes
 - daily [12-51](#)
 - application servers
 - hourly [12-51](#)
 - AS, daily [12-44](#)
 - GTT, daily [12-51](#)
 - MLR, daily [12-53](#)
 - MTP3, daily [12-44](#)
 - point code, inventory [12-58](#)
- exporting
 - data [5-38](#)
- exporting current MWTM data
 - for network objects [5-38](#)
 - node names [5-39](#)
 - SNMP community names [5-39](#)

F

- FAQs [C-1](#)
 - accounting [C-14](#)
 - applications, other [C-9](#)
 - asterisks [C-14](#)
 - browser [C-6](#)
 - capacity planning [C-20](#)
 - deployment [C-14](#)
 - discovery [C-13](#)

- events and alarms [C-7](#)
- HSRP [C-20](#)
- in-band management [C-18](#)
- installation [C-2](#)
- ITP reports [C-16](#)
- Java RMI [C-10](#)
- limited functionality [C-17](#)
- linkset totals [C-14](#)
- link totals [C-14](#)
- locked up display [C-5](#)
- MIBs [C-9](#)
- moving servers [C-3](#)
- out-of-band management [C-18](#)
- percentages [C-14](#)
- polling [C-8](#)
- rebooting [C-5](#)
- requirements [C-3](#)
- server communication [C-19](#)
- server messages [C-4, C-10](#)
- sounds [C-7](#)
- SSL, installing [C-5](#)
- status [C-10](#)
- superuser [C-10](#)
- syncing [C-20](#)
- syslog [C-10](#)
- text entry fields [C-5](#)
- timing service [C-8](#)
- topology maps [C-7](#)
- traps [C-13](#)
- uninstallation [C-2](#)
- user password [C-10](#)
- Windows [C-9](#)
- workstations [C-3](#)
- yellow nodes [C-22](#)
- features
 - customization [1-5](#)
 - GUI [1-2](#)
 - integration [1-5](#)
 - monitoring [1-3](#)

- navigational [4-17](#)
- performance [1-3](#)
- provisioning [1-3](#)
- security [1-4](#)
- server and network [1-2](#)
- topology [1-4](#)
- troubleshooting [1-4](#)
- web [1-2](#)

file

- node
 - MWTM panel [5-30](#)
 - panel [5-31](#)

file menu [4-21](#)

files

- ITP
 - deploying [5-36](#)
 - managing [5-25](#)
- loading [4-29](#)
- saving MWTM [4-29](#)

filtering view [7-9](#)

firewalls [H-6](#)

- configuring [H-8](#)

G

General commands

- mwtm datadir [B-22](#)

general commands [B-1](#)

- mwtm [B-5](#)
- mwtm addcreds [B-6](#)
- mwtm adduser [B-7](#)
- mwtm authtype [B-8](#)
- mwtm backup [B-9](#)
- mwtm backupdir [B-10](#)
- mwtm badloginalarm [B-11](#)
- mwtm badlogindisable [B-11](#)
- mwtm browserpath [B-12](#)
- mwtm certgui [B-12](#)
- mwtm certtool [B-12](#)

- mwtm changes [B-13](#)
- mwtm checksystem [B-13](#)
- mwtm clean [B-14](#)
- mwtm cleanall [B-14](#)
- mwtm cleandb [B-15](#)
- mwtm cleandiscover [B-16](#)
- mwtm cliconntimer [B-16](#)
- mwtm client [B-17](#)
- mwtm clientlogs [B-18](#)
- mwtm clitimeout [B-18](#)
- mwtm cmdlog [B-18](#)
- mwtm console [B-20](#)
- mwtm countnodes [B-20](#)
- mwtm countobjects [B-21](#)
- mwtm cwsetup [B-21](#)
- mwtm dbtool [B-23](#)
- mwtm delete [B-23](#)
- mwtm deletcreds [B-24](#)
- mwtm deluser [B-25](#)
- mwtm disablepass [B-25](#)
- mwtm disableuser [B-26](#)
- mwtm discover [B-26](#)
- mwtm diskmonitor [B-26](#)
- mwtm enableuser [B-27](#)
- mwtm eventautolog [B-27](#)
- mwtm eventconfig [B-28](#)
- mwtm eventeditor [B-28](#)
- mwtm eventtool [B-29](#)
- mwtm evilstop [B-30](#)
- mwtm export [B-30](#)
- mwtm export cw [B-31](#)
- mwtm help [B-32](#)
- mwtm inactiveuserdays [B-32](#)
- mwtm installlog [B-33](#)
- mwtm inventorytool [B-34](#)
- mwtm iosreport [B-35](#)
- mwtm ipaccess [B-35](#)
- mwtm jspport [B-36](#)
- mwtm keytool [B-36](#)

- mwtm killclients [B-37](#)
- mwtm listusers [B-37](#)
- mwtm logger [B-38](#)
- mwtm logtimemode [B-40](#)
- mwtm manage [B-40](#)
- mwtm maxascirows [B-42](#)
- mwtm maxevhist [B-42](#)
- mwtm maxhtmlrows [B-43](#)
- mwtm mldebug [B-43](#)
- mwtm motd [B-44](#)
- mwtm msglog [B-45](#)
- mwtm msglogage [B-45](#)
- mwtm msglogdir [B-46](#)
- mwtm msglogsize [B-39](#)
- mwtm netlog [B-46](#)
- mwtm netlogger [B-47](#)
- mwtm newlevel [B-47](#)
- mwtm osinfo [B-47](#)
- mwtm passwordage [B-47](#)
- mwtm patchlog [B-48](#)
- mwtm poll [B-49](#)
- mwtm pollertimeout [B-49](#)
- mwtm print [B-49](#)
- mwtm props [B-50](#)
- mwtm provisiontool [B-50](#)
- mwtm purgedb [B-51](#)
- mwtm readme [B-52](#)
- mwtm reboot [B-52](#)
- mwtm rep15minage [B-130](#)
- mwtm repdailyage [B-52](#)
- mwtm rephelp [B-53](#)
- mwtm rephourlyage [B-53](#)
- mwtm repmonthlyage [B-131](#)
- mwtm restart [B-53](#)
- mwtm restore [B-54](#)
- mwtm restoreprops [B-55](#)
- mwtm rootvars [B-55](#)
- mwtm sechelp [B-55](#)
- mwtm seclogmwtm seclog [B-55](#)
- mwtm secondaryserver [B-56](#)
- mwtm servername [B-57](#)
- mwtm setpath [B-57](#)
- mwtm showcreds [B-59](#)
- mwtm snmpcomm [B-59](#)
- mwtm snmpconf [B-60](#)
- mwtm snmpget [B-60](#)
- mwtm snmphelp [B-63](#)
- mwtm snmpnext [B-63](#)
- mwtm snmpwalk [B-66](#)
- mwtm sounddir [B-69](#)
- mwtm ssl [B-70](#)
- mwtm sslstatus [B-71](#)
- mwtm start [B-71](#)
- mwtm start client [B-71](#)
- mwtm start jsp [B-72](#)
- mwtm start pm [B-72](#)
- mwtm start web [B-72](#)
- mwtm status [B-72](#)
- mwtm stop [B-72](#)
- mwtm stopclients [B-73](#)
- mwtm stop jsp [B-73](#)
- mwtm stop pm [B-73](#)
- mwtm stop web [B-73](#)
- mwtm superuser [B-73](#)
- mwtm syncusers [B-74](#)
- mwtm tac [B-74](#)
- mwtm termproxy [B-75](#)
- mwtm trapaccess [B-75](#)
- mwtm trapsetup [B-76](#)
- mwtm trapstatus [B-77](#)
- mwtm tshootlog [B-77](#)
- mwtm uninstall [B-78](#)
- mwtm unknownage [B-78](#)
- mwtm updateuser [B-78](#)
- mwtm useraccess [B-79](#)
- mwtm userpass [B-79](#)
- mwtm version [B-80](#)
- mwtm viewlog [B-80](#)

- mwtm wall [B-80](#)
- mwtm webaccesslog [B-81](#)
- mwtm weberrorlog [B-81](#)
- mwtm weblogupdate [B-82](#)
- mwtm webnames [B-83](#)
- mwtm webport [B-83](#)
- mwtm webutil [B-84](#)
- mwtm who [B-84](#)
- mwtm xtermpath [B-84](#)
- generating
 - custom reports [12-3](#)
 - reports [12-1](#)
- getting started [4-1](#)
- GGSN
 - MIBS
 - specific [F-6](#)
 - traps [G-16](#)
- Global Title Translation (see GTT)
- go menu [4-25](#)
- GTT
 - address conversion [14-14](#)
 - selector table [14-15](#)
 - tab [14-13](#)
 - table [14-14](#)
 - address conversion table
 - adding [14-26](#)
 - entries, adding [14-28](#)
 - app group tab [14-10](#)
 - application groups
 - adding [14-23](#)
 - basic information [14-1, 14-38](#)
 - CPC
 - lists, adding [14-26](#)
 - tab [14-12](#)
 - tab, concerned pt code name list [14-13](#)
 - deploying [14-37](#)
 - editor
 - launching [14-2](#)
 - menu [14-4](#)
 - files
 - creating [14-30](#)
 - cross-instance [14-39](#)
 - editing [14-16](#)
 - export [12-51](#)
 - loading [14-31, 14-33](#)
 - loading from archive [14-34](#)
 - reverting [14-44](#)
 - saving [14-42](#)
 - GTA
 - entries, adding [14-18](#)
 - searching [14-21](#)
 - MAP
 - adding entries [14-24](#)
 - tab [14-11](#)
 - MAP status
 - viewing [8-125](#)
 - network name configuration [14-39](#)
 - menu [14-40](#)
 - table [14-41](#)
 - progress dialog [14-35](#)
 - reports, daily [12-41](#)
 - rows, deleting [14-29](#)
 - selectors
 - adding [14-17](#)
 - selectors and GTA tab [14-6](#)
 - CPC [14-10](#)
 - selectors and GTA table
 - app group [14-8](#)
 - GTA [14-8](#)
 - MAP [14-9](#)
 - selector [14-7](#)
 - semantics [14-36](#)
 - statistics
 - viewing [8-126](#)
- GTT accounting
 - reports [12-41](#)

H

HA

traps [G-19](#)

help menu [4-27](#)

home page

MWTM web interface [11-8](#)

HSRP

FAQs [C-20](#)

I

ignoring and unignoring

objects [6-43](#)

in-band management

FAQs [C-18](#)

including objects

ITP reports [12-4](#)

information

address [8-14](#)

bandwidth

RAN-O backhauls [8-15](#)

ITP

application servers [8-17](#)

linksets [8-18](#)

links [8-20](#)

naming

card [8-22](#)

interfaces [8-22](#)

ITP, application server process associations [8-23](#)

ITP, application server processes [8-23](#)

ITP, application servers [8-23](#)

ITP, linkset [8-24](#)

ITP, signaling-gateway mated pairs [8-24](#)

ITP, signaling points [8-24](#)

ITP links [8-23](#)

nodes [8-21](#)

polling

node [8-26](#)

protection

ONS nodes [8-27](#)

QoS

ITP signaling points [8-27](#)

RAN [8-27](#)

remote IP address [8-28](#)

status

interface and card [8-30](#)

ITP, application server process [8-35](#)

ITP application server process associations [8-36](#)

ITP application servers [8-34](#)

ITP links [8-38](#)

ITP linksets [8-39](#)

ITP signaling gateway mated pairs [8-40](#)

ITP signaling points [8-42](#)

node [8-29](#)

threshold (RAN-O only) [8-43](#)

uptime

node [8-28](#)

information, in a window

finding [5-23](#)

installation

FAQs [C-2](#)

integration

with CiscoWorks [5-39](#)

interface

tabs [A-11](#)

UMTS and GSM tabs (RAN-O only) [A-12](#)

interface and cardt

status

information [8-30](#)

interface content

MWTM web interface [11-4](#)

interfaces

naming

information [8-22](#)

packet size [8-17](#)

status definitions [E-8](#)

table [6-21](#)

- introduction to SGM [1-1](#)
- inventory
 - point code [6-31](#)
- IOS
 - commands, troubleshooting [D-4](#)
 - server load balancing [H-18](#)
- IP addresses accounting
 - reports [6-31](#)
- IP Transfer Point (see ITP)
- ITP
 - application server process
 - status, information [8-35](#)
 - application server processes
 - naming, information [8-23](#)
 - application servers
 - information [8-17](#)
 - naming, information [8-23](#)
 - status, information [8-34](#)
 - commands [B-85](#)
 - files
 - deploying [5-36](#)
 - managing [5-25](#)
 - linkset
 - naming, information [8-24](#)
 - linksets
 - information [8-18](#)
 - non-stop operation
 - viewing [8-95](#)
 - overview [1-6](#)
 - signaling gateway-mated pairs
 - naming, information [8-24](#)
 - signaling points
 - naming, information [8-24](#)
- ITP application server process associations
 - naming
 - information [8-23](#)
 - status
 - information [8-36](#)
- ITP commands
 - mwtm 15minage [B-131](#)
 - mwtm accstats [B-87](#)
 - mwtm archivedir [B-88](#)
 - mwtm atblclient [B-89, B-115](#)
 - mwtm atbldir [B-90](#)
 - mwtm autosynconfig [B-91](#)
 - mwtm chartwindow [B-91](#)
 - mwtm checkgtt [B-91](#)
 - mwtm checkmlr [B-92](#)
 - mwtm checkroute [B-92](#)
 - mwtm countas [B-92](#)
 - mwtm countasp [B-92](#)
 - mwtm countaspa [B-93](#)
 - mwtm countlinks [B-93](#)
 - mwtm countlinksets [B-93](#)
 - mwtm countsgrp [B-93](#)
 - mwtm countsps [B-93](#)
 - mwtm deletearchive [B-94](#)
 - mwtm deploarchive [B-94](#)
 - mwtm deplocomments [B-95](#)
 - mwtm evreps clean [B-95](#)
 - mwtm evreps cleancustom [B-95](#)
 - mwtm evreps diskcheck [B-95](#)
 - mwtm evreps enable [B-96](#)
 - mwtm evreps hourlyage [B-96](#)
 - mwtm evreps mtp [B-97](#)
 - mwtm evreps status [B-97](#)
 - mwtm evrepstimer [B-97](#)
 - mwtm gttclient [B-98, B-116](#)
 - mwtm gttmdir [B-98](#)
 - mwtm gttstats [B-100](#)
 - mwtm linkstats [B-101](#)
 - mwtm listarchive [B-103](#)
 - mwtm listgtt [B-103](#)
 - mwtm listhistory [B-104](#)
 - mwtm listmlr [B-104](#)
 - mwtm listroute [B-104](#)
 - mwtm maxcsvrows [B-123](#)
 - mwtm mlrstats [B-105](#)

- mwtm mtpevents [B-106](#)
- mwtm pformat [B-107](#)
- mwtm pclist [B-108](#)
- mwtm pushgtt [B-108](#)
- mwtm pushmlr [B-109](#)
- mwtm pushroute [B-110](#)
- mwtm q752stats [B-110](#)
- mwtm repcustage [B-112](#)
- mwtm repdir [B-112](#)
- mwtm replog [B-113](#)
- mwtm routedir [B-114](#)
- mwtm routetabledefs [B-115](#)
- mwtm stareps cleancustom [B-118](#)
- mwtm stareps diskcheck [B-119](#)
- mwtm stareps gtt [B-121](#)
- mwtm statreps acct [B-117](#)
- mwtm statreps clean [B-117](#)
- mwtm statreps custage [B-118](#)
- mwtm statreps dailyage [B-119](#)
- mwtm statreps enable [B-120](#)
- mwtm statreps hourlyage [B-121](#)
- mwtm statreps link [B-122](#)
- mwtm statreps mlr [B-123](#)
- mwtm statreps monthlyage [B-132](#)
- mwtm statreps msu [B-124](#)
- mwtm statreps nullcaps [B-125](#)
- mwtm statreps q752 [B-125](#)
- mwtm statreps servratio [B-126](#)
- mwtm statreps status [B-126](#)
- mwtm statreps timemode [B-127](#)
- mwtm statreps timer [B-127](#)
- mwtm statreps utilratio [B-128](#)
- mwtm statreps xua [B-128](#)
- mwtm xuastats [B-129](#)
- statreps export [B-120](#)
- statreps iplinks [B-122](#)
- ITP links
 - naming
 - information [8-23](#)
- status
 - information [8-38](#)
- ITP linkset
 - access lists
 - viewing [8-123](#)
- ITP linksets
 - status
 - information [8-39](#)
- ITP MIBS
 - specific [F-8](#)
- ITP MSU
 - errors, viewing [8-94](#)
- ITP MTP3
 - errors, viewing [8-93](#)
- ITP networks
 - discovery
 - dialog menu [4-6](#)
 - dialog tabs [4-6](#)
 - nodes [4-15](#)
 - running [4-12](#)
 - settings [4-13](#)
 - verifying [4-15](#)
- ITP reports
 - excluding objects [12-4](#)
 - FAQs [C-16](#)
 - including objects [12-4](#)
 - locating [12-63](#)
 - preferences [12-65](#)
- ITP signaling gateway mated pairs
 - status
 - information [8-40](#)
- ITP signaling point
 - description [8-16](#)
 - specific data, viewing [8-123](#)
- ITP signaling points
 - managing [6-42](#)
 - QoS
 - information [8-27](#)
 - status

information [8-42](#)
 unmanaging [6-42](#)
 ITP traps [G-7](#)

J

JAVA RMI
 FAQs [C-10](#)

L

launching
 discovery dialog [4-6](#)
 limited functionality
 FAQs [C-17](#)
 link
 configuration
 interfaces [8-18](#)
 reports
 daily [12-19](#)
 hourly [12-18](#)
 tabs [A-9](#)
 links
 configuration
 IP addresses [8-20](#)
 information [8-20](#)
 reports [12-17](#)
 five day [12-22](#)
 status definitions [E-6](#)
 table [6-13](#)
 linkset
 archived reports
 daily [12-53](#)
 hourly [12-53](#)
 description [8-16](#)
 reports
 daily [12-24](#)
 daily peaks [12-26](#)

hourly [12-23](#)
 table [6-10](#)
 tabs [A-9](#)
 linksets
 status definitions [E-7](#)
 linkset totals
 FAQs [C-14](#)
 link totals
 FAQs [C-14](#)
 Linux MWTM client, starting [4-3](#)
 locating
 ITP reports [12-63](#)
 locked up display
 FAQs [C-5](#)
 login credentials, setting up [3-20](#)

M

management interface folder
 tabs [A-13](#)
 managing
 event [9-1](#)
 ITP signaling points [6-42](#)
 nodes [6-42](#)
 reports [12-1](#)
 mapping files, network name [15-20](#)
 menu
 address tables [15-3](#)
 menus
 file [4-21](#)
 go [4-25](#)
 help [4-27](#)
 tools [4-25](#)
 messages
 display, changing [3-4](#)
 log file
 age [3-5](#)
 dates [3-5](#)
 location [3-4](#)

- log files
 - size [3-4](#)
 - of the day [2-16](#)
- MIBs
 - common [F-2](#)
 - FAQs [C-9](#)
- MLR
 - details
 - viewing [8-130](#)
 - export files, daily [12-53](#)
 - reports [12-27](#)
 - aborts [12-27](#)
 - continues [12-28](#)
 - daily [12-27](#)
 - processed [12-29](#)
 - result invokes [12-30](#)
 - rule matches [12-31](#)
 - subtriggers [12-31](#)
 - triggers [12-32](#)
- mobile Services Exchange Framework (see mSEF)
- Mobile Wireless Transport Manager (see MWTM)
- moving servers
 - FAQs [C-3](#)
- mSEF
 - overview [1-9](#)
 - traps [G-12](#), [G-13](#)
- MSU
 - archived reports
 - daily [12-55](#)
 - hourly [12-54](#)
 - load
 - reports [12-33](#)
 - peaks
 - reports [12-33](#)
 - rates
 - reports [12-32](#)
- MTP3
 - custom reports, accounting [12-57](#)
 - event log
 - viewing [8-129](#)
 - export files, daily [12-44](#)
 - reports
 - custom [12-57](#)
 - daily [12-42](#)
- MTP3 event
 - reports
 - detail [12-57](#)
- MTP3 event reports [12-55](#)
- multiple-instance ITPs, connecting [3-6](#)
- MWTM
 - about [iii-xxxi](#)
 - backup [2-32](#)
 - client and server communication
 - dynamic NAT [H-17](#)
 - firewalls [H-6](#)
 - NAT [H-5](#)
 - port-forwarding [H-12](#)
 - SSL [H-17](#)
 - TCP [H-17](#)
 - VPN [H-3](#)
 - integration [5-39](#)
 - ITP route table file
 - editing [13-1](#)
 - main menu, using [4-21](#)
 - main window [4-16](#)
 - MIB reference [F-1](#)
 - networking options (see MWTM, client and server communication) [H-1](#)
 - overview [1-1](#)
 - restoring [2-32](#)
 - sessions, running simultaneous [5-43](#)
 - traps, supported [G-1](#)
 - troubleshooting (see troubleshooting)
 - uninstalling [4-32](#)
 - web browser, accessing [4-28](#)
- MWTM process
 - events
 - changing [9-35](#)

MWTM server (see server, MWTM)

MWTM web interface

additional information [11-11](#)

archived messages

viewing [11-19](#)

home page [11-8](#)

interface content [11-4](#)

logs

command [11-23](#)

console [11-22](#)

event automation [11-23](#)

security [11-23](#)

web access [11-24](#)

web server error [11-24](#)

messages [11-16](#)

action [11-17](#)

error [11-16](#)

info [11-16](#)

MWTM client, downloading [11-9](#)

navigation tree [11-3](#)

software updates [11-11](#)

system

clients [11-21](#)

information [11-14](#)

status [11-21](#)

user accounts [11-21](#)

versions [11-21](#)

technical documentation [11-12](#)

MWTM windows

printing [5-25](#)

N

navigating

table columns [5-24](#)

navigational

features [4-17](#)

navigation tree

MWTM client [4-19](#)

MWTM web interface [11-3](#)

network

topology [10-1](#)

views

topology [10-1](#)

network name mapping files, creating [15-20](#)

network objects

viewing a summary [4-19](#)

node

access [4-4](#)

archive

management [5-33](#)

BWG

tabs [A-2](#)

CSG

tabs [A-3](#)

CSR

tabs [A-3](#)

file

management [5-26](#)

menu, management [5-27](#)

MWTM panel [5-30](#)

files

ITP panel [5-31](#)

GGSN

tabs [A-4](#)

HA

tabs [A-4](#)

ITP

tabs [A-5](#)

naming

information [8-21](#)

ONS

tabs [A-6](#)

polling

information [8-26](#)

RAN service module

tabs [A-7](#)

status

- information [8-29](#)
 - uptime
 - information [8-28](#)
- node and ONS card details window
 - configuration data
 - descriptive information [8-16](#)
- node details window
 - configuration data
 - IP addresses for SNMP [8-19](#)
- node name
 - settings [5-5](#)
- nodes
 - deleting
 - from MWTM discovery database [6-41](#)
 - excluding from view [6-43](#)
 - managing [6-42](#)
 - polling [8-53](#)
 - SNMP IP addresses
 - editing [8-51](#)
 - status definitions [E-1](#)
 - trap
 - processing [8-56](#)
 - unmanaging [6-42](#)
 - window [6-2](#)
 - menus, right-click [6-4](#)
 - node table [6-5](#)
- nodes and files, seed
 - loading [4-7](#)
- notes
 - attaching [6-38](#)
 - event [9-29](#)
 - viewing [6-39](#)

O

- object details window
 - configuration data
 - naming [8-21](#)
- object functions

- detailed
 - understanding [8-1](#)
- objectives
 - document [iii-xxxi](#)
- object map
 - reference [A-1](#)
- objects
 - deleting [6-40](#)
 - from MWTM database [6-40](#)
 - from network [6-40](#)
 - ignoring and unignoring [6-43](#)
- objects within a view
 - displaying [11-33](#)
- online help
 - viewing [5-22](#)
- ONS nodes
 - protection
 - information [8-27](#)
- operations
 - basic server
 - performing [5-43](#)
- organization
 - document [iii-xxxii](#)
- out-of-band management
 - FAQs [C-18](#)
- overview
 - discovery [4-4](#)

P

- pane
 - troubleshooting [5-6](#)
- passwords (see security)
- peak
 - reports
 - daily [12-21](#)
- percentages
 - FAQs [C-14](#)
- performance statistics

- displaying [11-34](#)
- performing
 - basic server operations [5-43](#)
- physical folder
 - tabs [A-13](#)
- point code
 - export files, inventory [12-58](#)
 - inventory [6-31](#)
 - reports [6-31](#)
 - setting format [3-5](#)
- poller
 - settings [5-6](#)
 - settings, changing [3-2](#)
- poller settings window [8-110](#)
- polling
 - FAQs [C-8](#)
 - nodes [8-53](#)
- port numbers and parameters
 - configuring [H-7](#)
- ports
 - MWTM [I-1](#)
- preferences
 - ITP reports [12-65](#)
 - menu
 - displaying [5-3](#)
 - settings
 - CiscoWorks server [5-13](#)
 - deploy [5-16](#)
 - troubleshooting [5-6](#)
- preference settings
 - default, restoring [5-19](#)
 - web
 - changing [5-20](#)
- printing
 - MWTM windows [5-25](#)
- products menu [4-25](#)
- properties
 - editing [6-33](#)
- provisioning

- prerequisites [8-49](#)
- using [8-46](#)
- wizard
 - using [8-50](#)

R

Radio Access Network Optimization (see RAN-O)

RAN

- information [8-27](#)

RAN backhaul

- table [6-25](#)

- tabs [A-13](#)

virtual

- creating [8-140](#)

RAN data export files

- displaying [11-43](#)

RAN-O

backhaul

- properties, editing [6-36](#)

MIBS

- specific [F-10](#)

- overview [1-8](#)

- traps [G-11](#)

RAN-O only

threshold

- information [8-43](#)

RAN shorthauls

- viewing [8-140](#)

README file [4-32](#)

real-time data

ITP objects

- viewing [8-66](#)

objects

- viewing [8-56](#)

real-time poller

settings

- changing [5-21](#)

rebooting

- FAQs [C-5](#)
- recent events
 - viewing [8-45](#)
- reference
 - command [B-1](#)
 - object map [A-1](#)
- remote IP address
 - information [8-28](#)
- report
 - event metrics
 - viewing [9-30](#)
- reports
 - application server [12-9](#)
 - application server processes
 - daily [12-13](#)
 - hourly [12-12](#)
 - application servers
 - hourly [12-9](#)
 - peaks [12-11](#)
 - archived
 - custom [12-46](#)
 - daily [12-48](#)
 - hourly [12-49](#)
 - rolling [12-49](#)
 - AS accounting [12-44](#)
 - ASP accounting [12-44](#)
 - custom (see custom reports)
 - directory [12-65](#)
 - displaying [11-33](#)
 - file archive [12-45](#)
 - generating [12-1](#)
 - GTT, daily [12-41](#)
 - GTT accounting [12-41](#)
 - IP addresses accounting [6-31](#)
 - link [12-17](#)
 - five day [12-22](#)
 - linkset [12-23](#)
 - log [12-59](#)
 - managing [12-1](#)
 - MLR [12-27](#)
 - aborts [12-27](#)
 - continues [12-28](#)
 - processed [12-29](#)
 - result invokes [12-30](#)
 - rule matches [12-31](#)
 - subtriggers [12-31](#)
 - triggers [12-32](#)
 - MSU load [12-33](#)
 - MSU peaks [12-33](#)
 - MSU rates [12-32](#)
 - MTP3, daily [12-42](#)
 - MTP3 accounting [12-42](#)
 - MTP3 event [12-55](#)
 - MTP3 events
 - custom [12-56](#)
 - hourly [12-55](#)
 - point code [6-31](#)
 - point code, inventory [6-31, 12-44](#)
 - system
 - parameters [12-59](#)
 - timers [12-59](#)
 - system log [11-25](#)
 - viewing [12-6](#)
- reports, accounting
 - viewing [12-41](#)
- reports, statistics
 - viewing [12-9](#)
- reports properties
 - viewing [11-29](#)
- requirements
 - FAQs [C-3](#)
- restoring
 - MWTM files [2-32](#)
- RMI
 - how does it work [H-2](#)
- root user, becoming [4-2](#)
- route detail
 - viewing [8-124](#)

- route table files [13-1](#)
 - deploying [13-13](#)
 - editing [13-5](#)
 - loading [13-12](#)
 - non-MWTM [13-16](#)
 - opening
 - from archive [13-4](#)
 - from file [13-2](#)
 - from ITP [13-3](#)
 - reverting to last saved [13-15](#)
- route table dialog
 - menu [13-7](#)
 - menus, right-click [13-8](#)
 - table [13-8](#)
- saving [13-13](#)

S

- sample firewall
 - configuration [H-10](#)
- saving
 - address table files [15-23](#)
 - alarm filter [9-26](#)
 - event filter [9-26](#)
 - GTT files [14-42](#)
 - MWTM files [4-29](#)
 - route table files [13-13](#)
 - seed files [4-8](#)
 - topology [10-18](#)
 - view [7-6](#)
- security [2-1](#)
 - client access, limiting [2-31](#)
 - data, restoring [2-19](#)
 - logs, system [2-18](#)
 - message of the day [2-16](#)
 - overview [2-1](#)
 - passwords
 - changing [2-14](#)
 - creating [2-7](#)
 - disabling, automatically [2-11](#)
 - disabling, manually [2-13](#)
 - re-enabling [2-14](#)
 - synchronizing [2-17](#)
- SSL [2-22](#)
 - enabling [2-22](#)
 - support, disabling [2-30](#)
 - support, managing [2-30](#)
- SSL certificates
 - details [2-29](#)
 - downloading [2-26](#)
 - exporting [2-28](#)
 - importing [2-27](#)
 - tool [2-26](#)
- superuser [2-20](#)
- user-based access
 - disabling [2-20](#)
 - implementing [2-2](#)
- user levels [2-7](#)
 - (level 1) basic user [2-8](#)
 - (level 2) power user [2-8](#)
 - (level 3) network operator [2-9](#)
 - (level 4) network administrator [2-9](#)
 - (level 5) system administrator [2-11](#)
- users
 - changing [2-14](#)
 - disabling, automatically [2-11](#)
 - disabling, manually [2-13](#)
 - listing current [2-18](#)
 - re-enabling [2-14](#)
- seed files
 - changing [4-11](#)
 - creating [4-10](#)
 - loading [4-7](#)
 - saving [4-8](#)
 - using a text editor [4-12](#)
- seed nodes, loading [4-7](#)
- semantics
 - address table files [15-17](#)

- GTT files [14-36](#)
- server
 - setting up [3-1](#)
- server, MWTM
 - changing default name [4-31](#)
 - connecting new [5-43](#)
 - IOS server load balancing [H-18](#)
 - removing data [2-35](#)
- server communication
 - FAQs [C-19](#)
- server configuration
 - MWTM [H-15](#)
- server messages
 - FAQs [C-4](#), [C-10](#)
- server properties
 - viewing [11-27](#)
- server status information
 - viewing [5-44](#)
- sessions, MWTM, running simultaneous [5-43](#)
- setting
 - alarm filter [9-18](#)
 - CiscoWorks server
 - changing [5-13](#)
 - deploy
 - changing [5-16](#)
 - event filter [9-18](#)
- settings
 - charts
 - changing [5-11](#)
 - connection [5-7](#)
 - event
 - changing [5-8](#)
 - exit [5-4](#)
 - general
 - display [5-4](#)
 - GUI
 - changing [5-4](#)
 - node name [5-5](#)
 - poller [5-6](#)
 - repaint [5-7](#)
 - startup [5-4](#)
 - status
 - changing [5-12](#)
 - topology
 - changing [5-14](#)
- severity
 - alarm [4-20](#)
- SGM
 - commands [B-1](#)
 - FAQs (see FAQs)
 - status definitions (see status, definitions)
- shorthaul
 - table [6-27](#)
- signaling gateway-mated pair
 - tabs [A-11](#)
- signaling gateway mated pairs
 - status definitions [E-7](#)
 - table [6-19](#)
- signaling point
 - tabs [A-8](#)
- signaling point details window
 - configuration data
 - capability point code [8-15](#)
 - point code [8-25](#)
- signaling points
 - status definitions [E-7](#)
 - window
 - signaling point information [6-8](#)
- single-instance ITPs, connecting [3-6](#)
- SNMP
 - settings
 - buttons [3-18](#)
 - commands [3-18](#)
 - configuring [3-15](#)
 - table [3-16](#)
 - trap, enabling [3-7](#)
- software versions
 - displaying [11-31](#)

- table [6-30](#)
- Solaris MWTM client, starting [4-3](#)
- sound files, adding [9-52](#)
- sound filters, event
 - creating new [9-50](#)
 - deleting [9-53](#)
 - listing for [9-49](#)
 - setting [9-49](#)
- sound filters, events
 - changing [9-53](#)
- sounds
 - FAQs [C-7](#)
- SSL (see also security)
- SSL, downloading module
 - from web server [2-24](#)
- SSL certificate tool, launching [4-32](#)
- starting MWTM
 - client [4-2](#)
 - server [4-1](#)
- startup
 - settings [5-4](#)
- statistics
 - archived reports
 - daily [12-52](#)
 - hourly [12-52](#)
- status
 - FAQs [C-10](#)
 - settings, changing [5-12](#)
- status color
 - definitions
 - application server process associations [E-4](#)
 - application server processes [E-4](#)
 - application servers [E-4](#)
 - interfaces [E-8](#)
 - links [E-6](#)
 - linksets [E-7](#)
 - nodes [E-1](#)
 - signaling gateway mated pairs [E-7](#)
 - signaling points [E-7](#)

- views [E-2](#)
- status contributors
 - viewing [8-10](#)
- Summary lists [4-20](#)
- summary lists [4-20, 11-31](#)
 - displaying [11-31](#)
- superuser [2-20](#)
 - FAQs [C-10](#)
- syncing
 - FAQs [C-20](#)
- syslog
 - FAQs [C-10](#)
 - viewing [8-57](#)
- system properties
 - viewing [11-25](#)

T

- table
 - application server process [6-16](#)
 - application server process associations [6-18](#)
 - application servers [6-14](#)
 - card [6-23](#)
 - interfaces [6-21](#)
 - linkset [6-10](#)
 - RAN backhaul [6-25](#)
 - RAN shorthaul [6-27](#)
 - signaling gateway mated pairs [6-19](#)
 - software versions [6-30](#)
- table columns
 - navigating [5-24](#)
- table file
 - address
 - loading [15-12](#)
- tabs
 - application server [A-9](#)
 - application server process [A-10](#)
 - application server process association [A-10](#)
 - BWG node [A-2](#)

- card [A-12](#)
- CSG node [A-3](#)
- CSR node [A-3](#)
- GGSN node [A-4](#)
- HA node [A-4](#)
- interface [A-11](#)
 - UMTS and GSM (RAN-O only) [A-12](#)
- ITP node [A-5](#)
- link [A-9](#)
- linkset [A-9](#)
- management interface folder [A-13](#)
- ONS node [A-6](#)
- physical folder [A-13](#)
- RAN backhaul [A-13](#)
- RAN service module node [A-7](#)
- signaling gateway-mated pair [A-11](#)
- signaling point [A-8](#)
- technical documentation (see MWTM web interface)
- terminal
 - enabling proxy [3-11](#)
- text entry fields
 - FAQs [C-5](#)
- TFTP
 - server (ITP only), setting up [3-12](#)
- timing service
 - FAQs [C-8](#)
- toplogy maps
 - FAQs [C-7](#)
- topology
 - centering [10-17](#)
 - color [10-22](#)
 - directories [10-19](#)
 - hiding [10-26](#)
 - icons, locking [10-25](#)
 - layouts, creating custom [10-16](#)
 - magnetic grid [10-20, 10-21](#)
 - map [10-10](#)
 - map menu [10-15](#)
 - menu [10-3](#)
 - network [10-1](#)
 - objects
 - aligning [10-24](#)
 - details [10-18](#)
 - excluded [10-10](#)
 - finding [10-16](#)
 - hiding [10-25](#)
 - new [10-9](#)
 - redrawing [10-26](#)
 - printing [10-18](#)
 - RAN-O [10-6](#)
 - redrawing [10-26](#)
 - restoring [10-27](#)
 - saving [10-18, 10-26](#)
 - settings
 - changing [5-14](#)
 - toolbar buttons [10-4](#)
 - viewing [10-1](#)
 - views menu [10-15](#)
- trap
 - event, forwarding [9-48](#)
 - IP address, limiting by [3-9](#)
 - nodes, processing [8-56](#)
 - server, forwarding [5-42](#)
 - settings
 - viewing [8-62](#)
 - SNMP, enabling [3-7](#)
- TRAP_RATE_ABATE_OFFSET [9-3](#)
- TRAP_RATE_LIMIT_COUNT [9-3, 9-4](#)
- trap forwarding properties
 - viewing [11-30](#)
- traps
 - FAQs [C-13](#)
 - supported, SGM [G-1](#)
- troubleshooting [8-43](#)
 - data [D-1](#)
 - diagnosing ITP problems [D-5](#)
 - diagnosing RAN-O problems [D-8](#)
 - error messages [D-2](#)

- data model mediator service [D-2](#)
- demand poller manager service [D-2](#)
- events [D-5](#)
- IOS commands [D-4](#)
- locked up display [D-1](#)
- logs [D-3](#)
- pane [5-6](#)
- server processes [D-3](#)
- web pages [D-4](#)

U

- uninstallation
 - FAQs [C-2](#)
- uninstalling MWTM [4-32](#)
- unmanaging
 - ITP signaling points [6-42](#)
 - nodes [6-42](#)
- user-based access (see security)
- user password
 - FAQs [C-10](#)
- users (see security)
- using
 - MWTM main menu [4-21](#)
 - provisioning [8-46](#)
 - Windows Start menu [4-30](#)

V

- view
 - basic information [7-2](#)
 - client-specific [7-15](#)
 - creating [7-8](#)
 - creating (see view editor window)
 - custom [7-2](#)
 - data panel [7-13](#)
 - default [7-2](#)
 - loading [7-14](#)

- detailed information
 - viewing [7-5](#)
 - directory listing panel [7-14](#)
 - displaying new objects [7-12](#)
 - editing [7-6](#)
 - excluding objects from [7-12](#)
 - ignoring [7-16](#)
 - including objects in [7-12](#)
 - listing
 - defined [7-13](#)
 - subfolders [7-14](#)
 - subviews [7-13](#)
 - list panel [7-13](#)
 - managing [7-1](#)
 - right-click menu [7-3](#)
 - saving [7-6](#)
 - table [7-3](#)
- view editor window [7-8](#)
 - closing [7-14](#)
 - left pane [7-10](#)
 - menu [7-9](#)
 - objects, right-click menu [7-11](#)
 - views, right-click menu [7-11](#)
- viewing [8-43](#)
 - accounting reports [12-41](#)
 - alarms [8-45](#)
 - details [8-12](#)
 - error data [8-115](#)
 - MLR
 - details [8-130](#)
 - MTP3
 - event log [8-129](#)
 - notes [6-39](#)
 - online help [5-22](#)
 - RAN shorthauls [8-140](#)
 - recent events [8-45](#)
 - reports [12-6](#)
 - route detail [8-124](#)
 - server properties [11-27](#)

- server status information [5-44](#)
- statistics reports [12-9](#)
- status contributors [8-10](#)
- syslog [8-57](#)
- system properties [11-25](#)
- topology [10-1](#)
- trap forward properties [11-30](#)
- troubleshooting [8-43](#)
- web configuration properties [11-27](#)
- viewing reports properties [11-29](#)
- views
 - status definitions [E-2](#)

W

- web configuration properties
 - viewing [11-27](#)
- web pages
 - metrics
 - dates [9-34](#)
 - day [9-33](#)
 - files [9-34](#)
 - severity [9-31](#)
 - status [9-32](#)
 - traps [9-33](#)
 - types [9-31](#)
 - SNMP trap
 - messages/day table [9-34](#)
 - status change
 - messages/day table [9-34](#)
 - troubleshooting [D-4](#)
- web preference, settings
 - changing [5-1](#)
- web server
 - downloading SSL module [2-24](#)
- Windows
 - FAQs [C-9](#)
- Windows Start menu
 - changing default

- MWTM server name [4-31](#)
- launching
 - DOS prompt [4-31](#)
 - MWTM client [4-31](#)
 - MWTM event editor [4-31](#)
 - MWTM README file [4-32](#)
 - SSL Certificate Tool [4-32](#)
- uninstalling MWTM [4-32](#)
- using [4-30](#)

Y

- yellow nodes
 - FAQs [C-22](#)

