Release Notes for the Cisco Mobile Wireless Transport Manager 6.0.2

Date: March 2007

These release notes describe the caveats for the Cisco Mobile Wireless Transport Manager (MWTM), Release 6.0.2. These release notes accompany the:

- *User Guide for the Cisco Mobile Wireless Transport Manager 6.0*
- *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.0*
- *OSS Integration Guide for the Cisco Mobile Wireless Transport Manager 6.0*

Note   You can access the most current Cisco documentation, including these release notes, online at:
http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html

For the latest MWTM information and software updates, go to http://www.cisco.com/go/mwtm.

Contents

These release notes contain:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

These release notes describe caveats, known bugs, and other important information for installing and using MWTM 6.0.2.

What's New in MWTM 6.0.2

The MWTM 6.0.2 release provides these new features:

Feature	Description
CPU memory utilization	Viewing CPU memory statistics for a selected node.
Cisco Data for Telecommunications (CDT) for number portability	Discovery of CDT and ability to launch its web URL.
Content Services Gateway 2 (CSG2) support	Support for the CSG2 on the Service and Application Module for IP (SAMI). Includes discovery, alarm support, troubleshooting, and viewing real-time statistics.
Interface statistics	Viewing interface performance and errors for a selected interface.
Support for new Radio Access Network-Optimized (RAN-O) cards in Cisco MWR-1941-DC-A	Support for these new RAN-O cards: NM-1A-OC3SMI, NM-1A-T3 and NM-16ESW
Support for Cisco 3825 router	Support for the Cisco 3825 router for RAN-O and Pseudowire Emulation Edge-to-Edge (PWE3). Includes discovery, troubleshooting, and alarm support. Also includes real-time and historical statistics for RAN-O.
Monitoring of Access Services Network Gateway (ASN-GW) for WiMax	Support for the ASN-GW on the SAMI and Cisco 7301. Includes discovery, troubleshooting, alarm support, and viewing real-time statistics.
Support for enhanced Home Agent (eHA)	Support for eHA on the SAMI. Includes discovery, troubleshooting, and alarm support.
Basic support for Time Division Multiplex (TDM) drop and insert	Viewing statistics for TDM E1 and T1 interfaces. Also includes alarm support.
Support for launching third-party software from MWTM	Support for launching to URLs of third-party software for OSS integration.
Monitoring of PWE3	Basic troubleshooting and trap support for PWE3.
ITP event help update	Updated the event-related help files for ITP events.
Change to industry-standard alarm style	Improved MWTM alarm and event GUIs that more closely align with the X.733 alarm standard.

Feature	Description
Support for new ITP software releases	• 12.4(11)SW3 • 12.2(25)SW11 • 12.2(18)IXD1 • 12.4(15)SW • 12.2(25)SW12 • 12.2(18)IXE
Support for new CSG2 releases	• 12.4(11)MD1 • 12.4(11)MD2
Support for new MWR and Cisco 3825 software releases	• 12.4(12)MR2, 12.4(16)MR (MWR) • 12.4(16)MR1 (MWR and Cisco 3825)
Support for new RAN-SVC module release	• 12.2(29)SM2
Support for new HA release	• 12.4(15)XM
Support for new GGSN releases	• 12.4(2)XB6 • 12.4(2)XB7
Support for new ASN-GW release	• 12.4(15)XL1

Installing the MWTM 6.0.2 Patch

The following MWTM 6.0.2 build files are available:

- Solaris—*mwtm602-sol-<date>-patch.zip*
- Linux—*mwtm602-linux-<date>-patch.zip*

For instructions on how to install the MWTM 6.0.2 patch build, refer to the *README-PATCH.txt* file included in the MWTM 6.0.2 patch at the software download site:

http://www.cisco.com/pcgi-bin/tablebuild.pl/mwtm

Use the supported path to upgrade to MWTM 6.0.2:

Current Installation	Upgrade Path
Signaling Gateway Manager (SGM) 4.1.*x*	**1.** Install MWTM 6.0.
MWTM 5.0.*x*	**2.** Install the MWTM 6.0.2 patch.
MWTM 6.0	**1.** Install the MWTM 6.0.2 patch.
MWTM 6.0.1	**1.** Install the MWTM 6.0.2 patch.

Limitations and Restrictions

This section describes limitations and restrictions that are associated with the MWTM:

Provisioning Timeout

When using the MWTM provisioning feature to modify the management interface, sometimes the operation fails with this message:

```
No prompt response
```

This response can occur when changing the *duplex* or *speed* attributes for the Ethernet interface. The response can also occur for other interface attributes that affect IP connectivity between the MWTM and the device.

The default setting for a provisioning operation timeout is 50 seconds. As a workaround, the system administrator can increase the TGS_OP_TIMEOUT attribute in the *System.properties* file to a higher value. You must restart the MWTM server for this change to take effect.

SSH-Enabled Nodes

The MWTM Node > Home Page right-click menu option does not work correctly for the following SSH-enabled IP Transfer Point (ITP) nodes:

- Cisco 2600
- Cisco 7200
- Cisco 7300
- Cisco 7500
- Cisco 7600

The browser launches, as expected, but the user is not prompted for login information.

Note This limitation exists for any ITP node running the 12.2(*x*) IOS with SSH enabled.

INSTANCE_NUMBER on Single-Instance ITP

Symptom If a command with INSTANCE_NUMBER is included in the *UserCommands.ts* file, the instance number will appear on all nodes in the GUI. If you run this command on a node that does not have multi-instance enabled, it fails.

Workaround If you have a network with both single-instance and multi-instance nodes, you must configure a separate set of troubleshooting commands for each node type in the *UserCommands.ts* file. Do this by grouping the commands for each type under a separate category.

Multiprocessor Multithread Vendor Exception

Sometimes when using the MWTM client on a Solaris multi-processor computer, an exception occurs when the topology window is open and you are manipulating views. The workaround is to close the topology window, then reopen it.

External SSH Client Use

If you enable the MWTM terminal proxy (**mwtm termproxy**) and use an external SSH terminal client to connect to a device, you might receive a warning message indicating a man-in-the-middle attack. This warning occurs because the MWTM server is operating as an SSH proxy to the device. In this scenario, ignore any warning messages indicating a man-in-the-middle attack. These warnings do not occur if you disable the MWTM terminal proxy or if you use the SSH terminal included with the MWTM.

CPU and Memory Utilization Statistics

Previous releases of the MWTM provided real-time charts that showed CPU utilization averaged over 5-second, 1-minute, and 5-minute intervals. These charts were accessible from a right-click menu after selecting a node in the navigation tree. Process-level CPU utilization was available in a multitabbed table under the CPU Utilization tab on the node details panel.

In MWTM 6.0.2, the CPU Utilization tab is renamed the Performance tab and shows real-time values. This tab contains selectable views for the CPU utilization chart, the process-level utilization table, and a new memory utilization table (see Figure 1). The node right-click menu option is no longer needed and has been removed.

Figure 1   New Performance Tab with Selectable Views
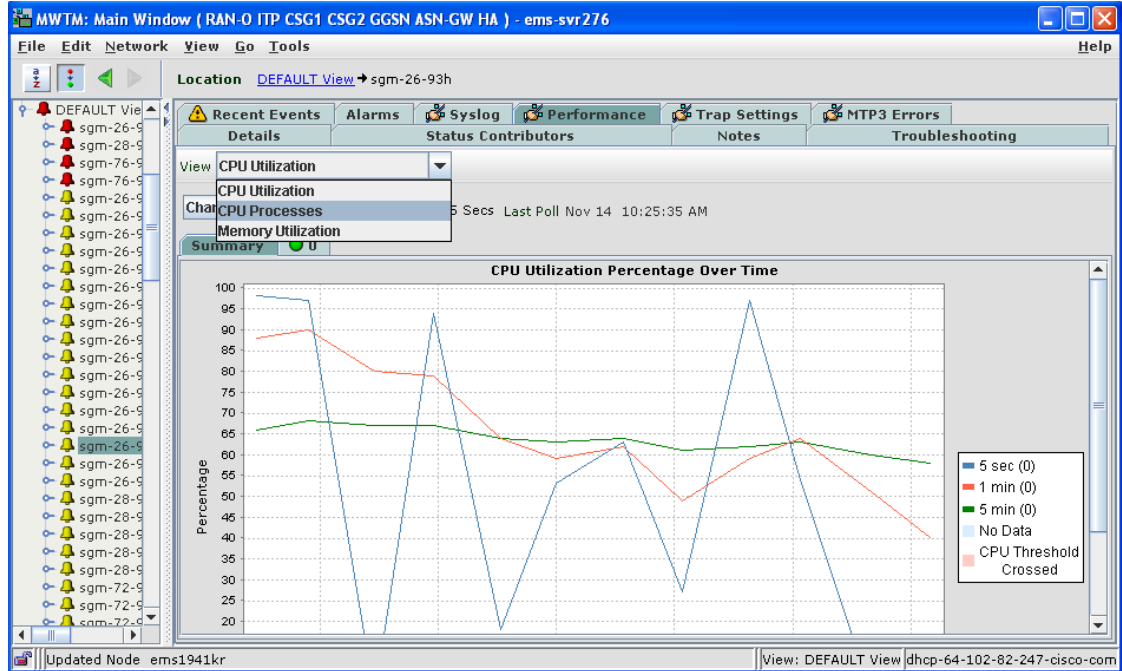
The memory utilization table displays a Summary tab with processor memory utilization and input/output (I/O) memory utilization for each CPU (see Figure 2). This table also has a tab for each CPU on the node. Clicking on a CPU-specific tab displays the utilization and memory for the selected CPU.

Depending on the node, memory utilization statistics may not be available from the Management Information Base (MIB). Nodes that support the CISCO-ENHANCED-MEMORY-POOL-MIB have detailed memory information for each CPU. Nodes that support the CISCO-MEMORY-POOL-MIB have memory information only for the CPU of the main processor. For these nodes, the memory utilization table shows only one entry even though these nodes can have multiple CPUs. In these cases, the CPU Description column indicates *CPU of main processor* as shown in Figure 2.

Figure 2   Memory Utilization Table

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. Nodes that support the CISCO-MEMORY-POOL-MIB show only the description of the main processor.

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 MEMORY_POLLER_TIMEOUT_INCREMENT in the *System.properties* file.

To display CPU thresholds on the MWTM, you must configure rising and falling thresholds on the devices themselves. The MWTM does not display CPU thresholds if these settings are absent.

Viewing Real-Time Data for Interfaces

Release 6.0.2 introduces the capability to view real-time data for interfaces that you select in the navigation tree. 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 selected 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.

Trap Configuration for CDT 2.0

CSCsk60334

If you configure Cisco Data Telecommunications (CDT) 2.0 for use with the MWTM, you must set up CDT 2.0 to send traps that conform to Trap Version 2 (V2 style). Do not configure CDT 2.0 to send traps that use Trap Version 1 style.

Launching Service Managers from MWTM

CSCsl17461

When you set the MWTM personalities to manage CSG and GGSN nodes, the MWTM Tools menu provides these launch commands in the MWTM client:

- Tools > CiscoWorks > CSG Service Manager
- Tools > CiscoWorks > GGSN Service Manager

Note In the MWTM web interface, you click CiscoWorks in the navigation tree, then click CSG or GGSN in the right pane to launch the service manager.

When you launch one of these commands, the MWTM attempts to launch the URL of the service manager that resides on the LMS server to which your MWTM client is currently connected. However, if the service manager is not actually 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 to which you are connected. Otherwise, you should remove the CSG or GGSN personality setting with the **mwtm manage** command (see mwtm manage, page 18).

Online Help System

The online help system is updated only during major release updates. New features added in patch releases (for example, in 6.0.2) are not contained in the online help system. Instead, new features are documented in the release notes for the patch release.

Important Notes

This section contains important notes about:

- Alarm Style Changes, page 8
- RAN Backhaul Utilization, page 16
- CLI Updates, page 16

Alarm Style Changes

MWTM 6.0.2 introduces a new alarm style that more closely conforms to the X.733 standard for alarms. The new alarm style is available in the MWTM Java client and the MWTM web interface.

While the new alarm style represents a change in MWTM alarm management for existing customers, the improvements of the new alarm style will facilitate alarm management and integration of MWTM alarms with northbound OSS interfaces.

This section describes the:

- Old Alarm Style, page 8
- New Alarm Style, page 9

Old Alarm Style

Figure 3 shows the Alarms table of the old alarm style of previous versions of the MWTM.

Figure 3   *Old Style Alarms Table*

As Figure 3 shows, the old alarm style did not provide key components important to alarm management, including the alarm name, alarm severity, the capability to acknowledge or clear alarms, and alarm filtering.

The old alarm style also lacked object-specific alarm information. Figure 4 shows multiple tabs for the selected object, but no Alarms tab.

Figure 4 **No Alarms Tab for Selected Object**
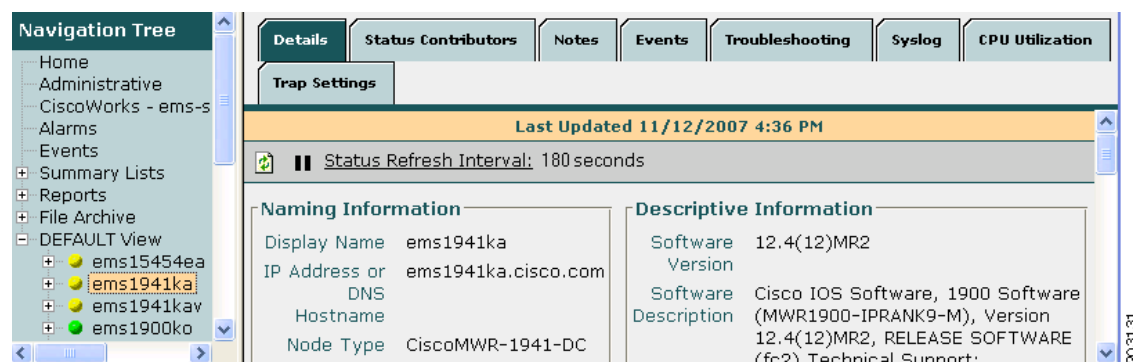
Also, the navigation tree of pre-6.0.2 MWTM versions featured colored balls to indicate the status of objects (but not their alarm severity). In addition, the old alarm style used nonstandard colors.

New Alarm Style

The new alarm style introduced in MWTM 6.0.2 provides industry-standard alarm attributes, a northbound API, improved synchronization of alarms between the OSS and the MWTM, and customization of alarm severity and message text. This new alarm style enables the MWTM to communicate alarms to northbound OSS interfaces through the alarm API. Also, future releases of MWTM will be able to support a broader range of alarms for ITP, RAN-O, CSG, GGSN, HA, and ASN Gateway nodes.

The MWTM 6.0.2 release includes these new alarm features:

- Basic Concepts and Terms, page 10
- Alarm Summary, page 11
- Active Alarms Table, page 12
- Alarm State Aggregation, page 12
- Alarm Filtering, page 13
- Alarm Customization, page 13
- Alarm Clearing, page 14
- Alarm Preferences, page 15

✎
Note These alarm features are available in the MWTM Java client and MWTM web interfaces, unless otherwise noted.

Basic Concepts and Terms

The new alarm style feature introduces these concepts and terms:

- Event Definition
- Alarm Definition

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

Events are written to the MWTM database once and never change. 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 related 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 5 shows an example of a sequence of related events that describe the lifecycle of one alarm.

Figure 5   Example of Alarm
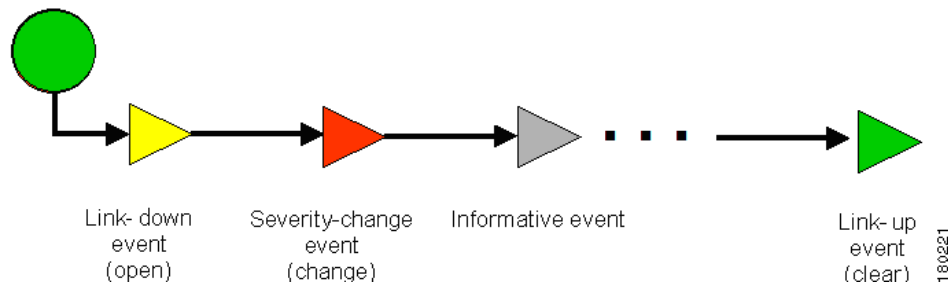
A complete event sequence for an alarm includes a minimum of two events:

- 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 related events that are triggered by changes in severity, updates to services, and so on. To view all alarms, click **Active Alarms** in the navigation tree.

Note   While some events correlate to a single alarm, some events do not raise alarms at all.

Alarm Summary

The MWTM 6.0.2 release displays a summary list of alarm counts by severity for all the nodes that the MWTM manages (see Figure 6). This high-level view allows operators to monitor the overall health of the MWTM-managed network. Figure 6 also shows the new alarm icon (bell) and colors to indicate the alarm severity of MWTM-managed objects. Figure 7 shows a summary of alarms for each managed node in the network.
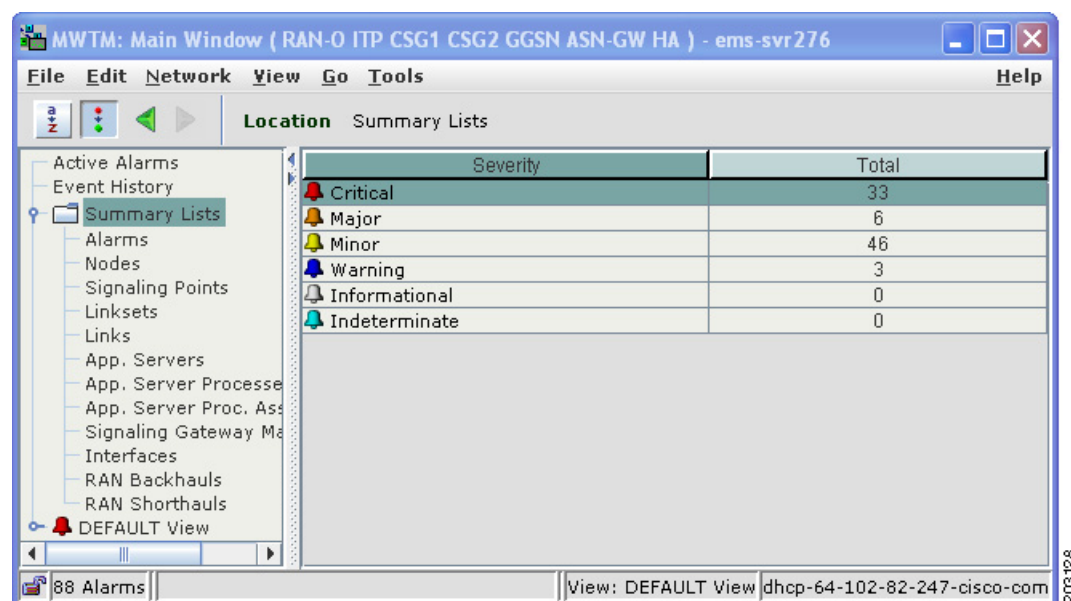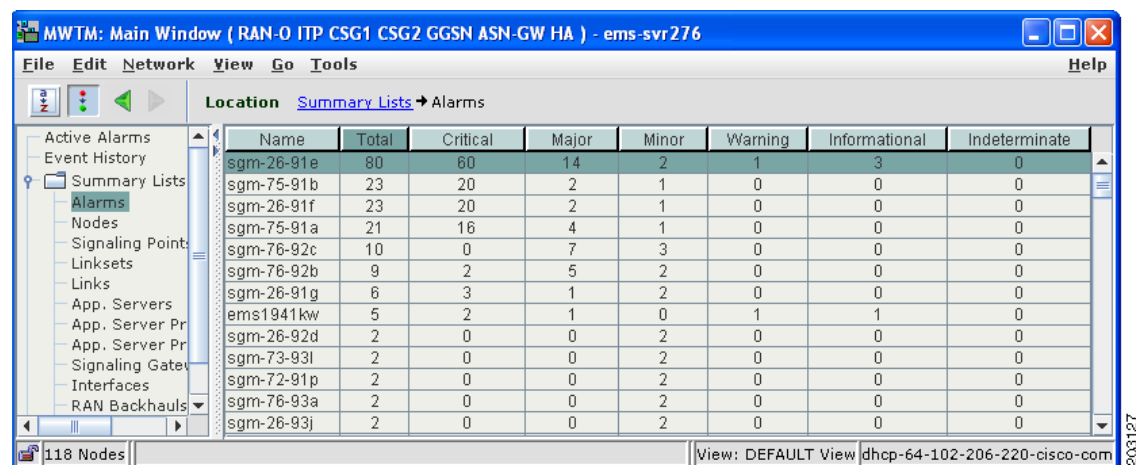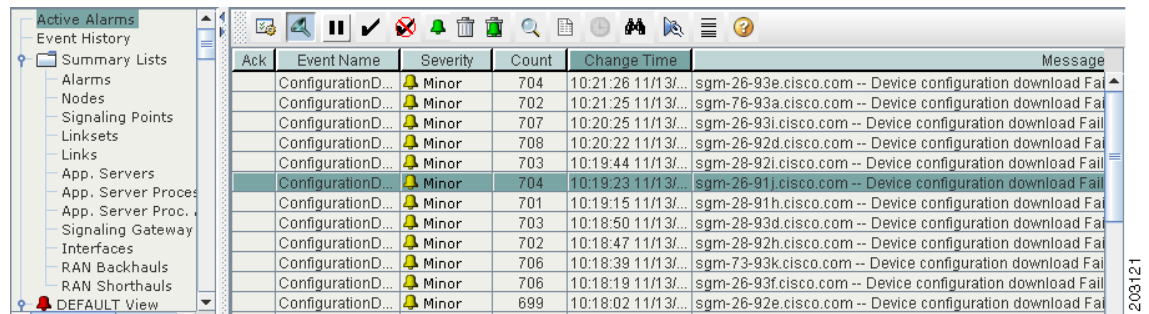
Figure 6   *Summary Lists*

Figure 7   *Alarms Summary*

Active Alarms Table

The Active Alarms table (Figure 8) features new attributes such as the alarm name, severity, message text, change time (the most recent event correlated to the alarm), and count (a running total of the number of events associated with the alarm).

Figure 8   ***Active Alarms Table***

Alarm State Aggregation

Figure 9 shows the new alarm icon and colors to indicate the alarm severity of objects in the navigation tree.

The navigation tree shown in Figure 9 also illustrates the concept of alarm state aggregation. The color of any object in the tree represents the highest (most critical) alarm severity of any of its subtending objects. In this example, several links are shown to have a critical severity. The MWTM propagates the most severe alarm to the highest object in the hierarchy. In this case, the severity of the link is propagated to the parent linkset, the parent signaling point, and finally the parent node. This presentation more accurately reflects the status of a node and its subtending objects.

Figure 9   ***Alarm State Aggregation***
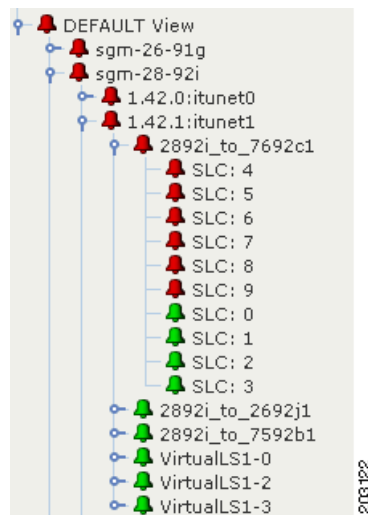
Alarm Filtering

The Filter dialog box shown in Figure 10 enables you to filter the alarms that the MWTM displays for selected objects. Note the use of different colors to indicate alarm severities.

Figure 10   *Alarm Filter*
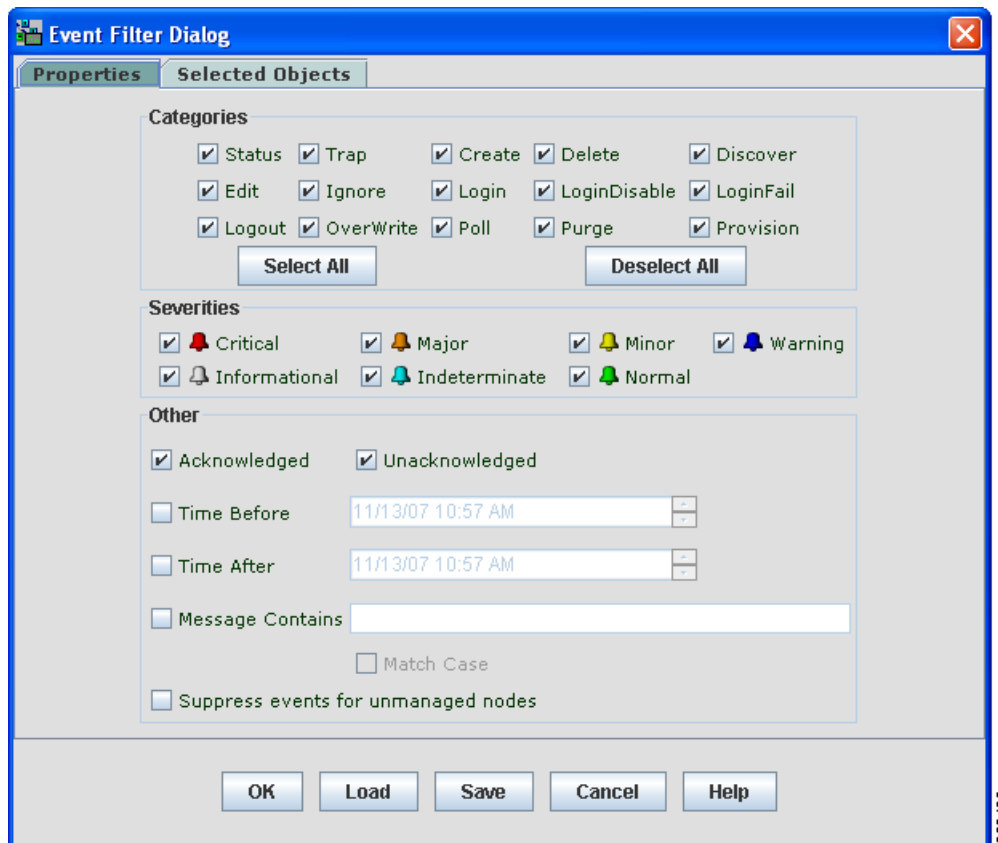
Alarm Customization

The new alarm model allows you to customize alarms (see Figure 11) by changing parameters such as alarm severity, alarm message text, whether the selected event should raise an alarm, and the event type or category that triggers the alarm.

Figure 11   Alarm Customization (Java Client Only)
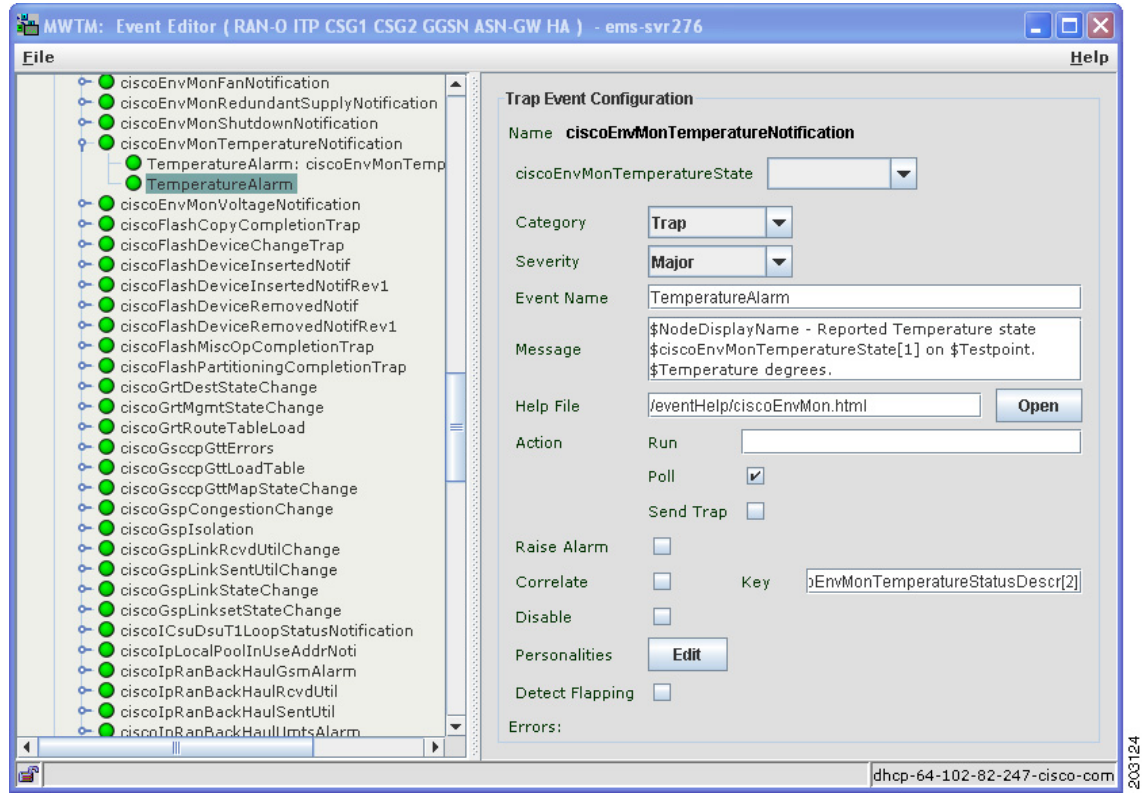
Alarm Clearing

The new alarm model enables you to acknowledge alarms, clear them (which changes the severity to normal), or clear and delete them (which also removes the alarm from view and archives it). These functions are available in the toolbar and the right-click menu for the selected alarm. See Figure 12.

Figure 12   Alarm Clearing Capability
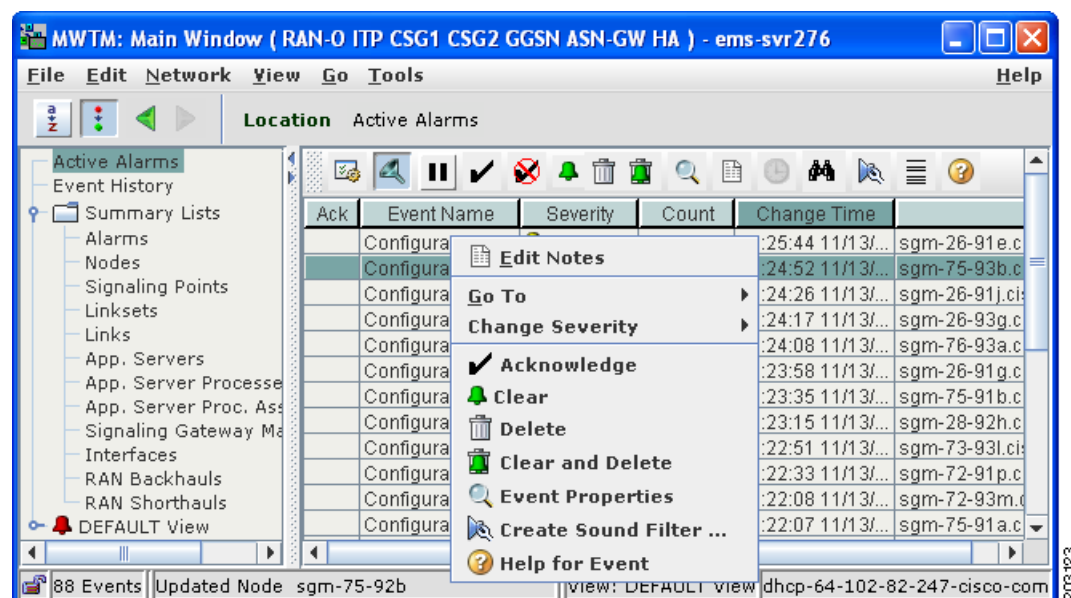
Alarm Preferences

The default settings for alarm severity include commonly accepted alarm colors. However, if required, you can change these colors through the Preferences window (Figure 13). You can also change the default color for nodes that the MWTM shows in its navigation tree and topology window but does not directly manage (unmanaged nodes).

Figure 13   Alarm Preferences (Java Client Only)
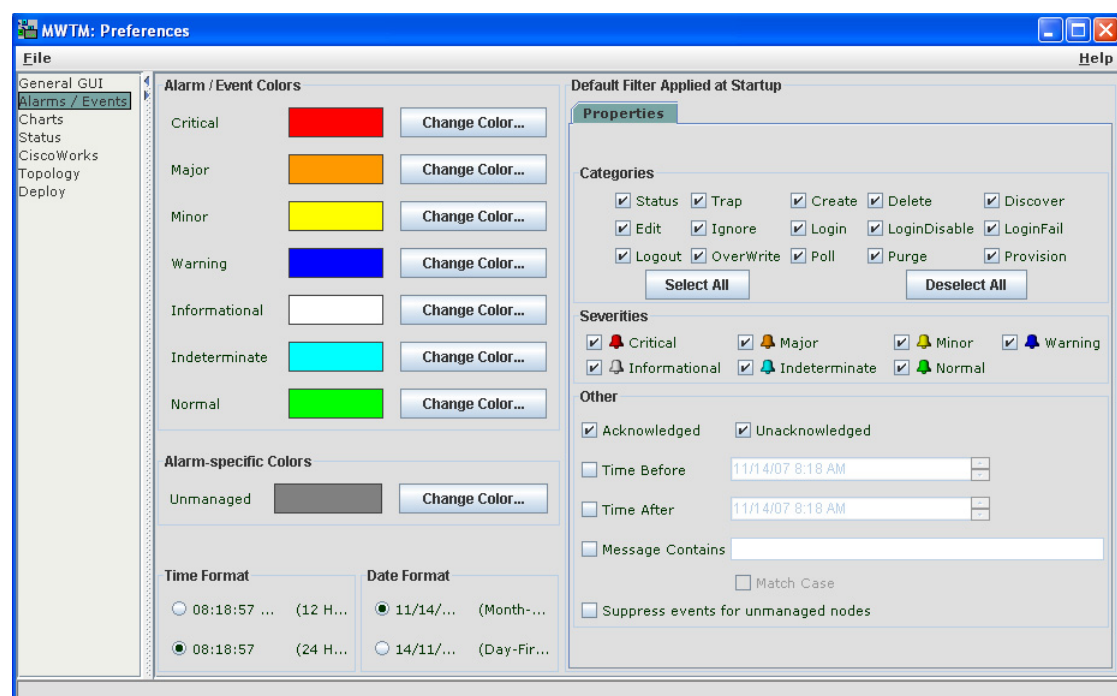
RAN Backhaul Utilization

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.

CLI Updates

MWTM 6.0.2 provides these commands and improvements:

- mwtm collectstats, page 16
- mwtm print, page 17
- mwtm iosreport, page 17
- mwtm trapratelimit, page 18
- mwtm importcw, page 18
- mwtm manage, page 18
- mwtm snmpsetup, page 19
- mwtm cwsetup, page 19
- Improved Command Prompting, page 20

mwtm collectstats

Full Syntax

mwtm collectstats [**-h** *hostname(s)*] {**-d** *date(s)* | **-s** *startdate* **-e** *enddate*} [**clean**]

Command Description

Gathers information from the *opt/CSCOsgm/logs/netstatus* and */opt/CSCOsgm/report/* folders. The mwtm collectstats output appears:

/opt/CSCOsgm/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** *startdate* and **-e** *enddate*— Collects reports and events for the devices indicated from a start date to an end date. The date format must be in YYYYMMDD. For example:

  `./mwtm collectstats -h hostname1 hostname2 hostname3 -s 20070621 –e 20070622`

- **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-<NameOfLog>.csv
cisco-mwtm-stats-event-trap-<NameOfLog>.csv
```

In addition, the MWTM creates a consolidated log file for all events and reports data separately.

You must log in as the root user or superuser to use this command.

mwtm print

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**—Prints only the alarm counts (without the severity label)
- **all**—Prints the information available for all of the keywords of this command.

You must log in as the root user or superuser to use this command.

mwtm iosreport

Full Syntax
mwtm iosreport

Command Description
Creates 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 trapratelimit

Full Syntax

mwtm trapratelimit {**count** | **interval**}

Command Description

Sets the trap rate limit for nodes or the time interval that the MWTM uses to determine if nodes are generating excessive traps.

Use these keywords with this command:

- **count**—Sets the trap limit for MWTM-managed nodes. The default setting is 2000 traps.

- **interval**—Sets the trap limit interval in minutes. The default setting is 30 minutes.

When you use the default settings, a node that generates 2000 or more traps within a 30-minute interval is considered to be generating too many traps (a trap storm). The MWTM stops trap processing for this node. After correcting the problem with the node, if you want to re-enable trap processing:

1. In the MWTM client, right-click the node in the navigation tree.

2. Choose **Allow Trap Processing** from the right-click menu.

You must log in as the root user or superuser to use this command.

You must restart the MWTM server for these changes to take effect.

mwtm importcw

Full Syntax

mwtm importcw [*cwfile*]

Command Description

Imports node hostname and read-community strings from the CiscoWorks server to the MWTM.

cwfile—Filename of the CiscoWorks export file (for example, */tmp/export.txt*). The export file 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 manage

✎
Note   Run this command to enable the ASN Gateway and HA nodes, which are added in Release 6.0.2.

Full Syntax

mwtm manage [**itp** | **ran-o** | **csg1** | **csg2** | **ggsn** | **asn-gw** | **ha**] [**enable** | **disable** | **status**]

Command Description

Enables, disables, or checks the status of one or more managed networks:

- **itp**, **ran-o**, **csg1**, **csg2**, **ggsn**, **asn-gw**, or **ha**—Type of network (or personality).

- **disable**—Disables the MWTM from managing the selected network.

- **enable**—Enables the MWTM to manage the selected 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 snmpsetup

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.

mwtm cwsetup

Note You must run **mwtm cwsetup uninstall**, then run **mwtm cwsetup install** because a new security field was added to the CiscoWorks preferences. (You will be prompted to indicate whether CiscoWorks security is enabled.)

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.

- If you do not include a keyword when you enter **mwtm cwsetup**, the command prompts you to enter the following information:
  - CiscoWorks server name
  - Port number for the CiscoWorks web server (the default setting is 1741)
  - Secure port number for the CiscoWorks web server (the default setting is 443)
  - Whether 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 the *User Guide for the Cisco Mobile Wireless Transport Manager 6.0*).

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.

Improved Command Prompting

The mwtm gttdir, mwtm atbldir, and mwtm routedir commands now have improved prompting to make them more user-friendly. The command scripts include improved prompting for TFTP parameters and creating the staging directory.

Resolved MWTM Caveats

The following bugs have been fixed in MWTM 6.0.2:

Bug ID	Description
CSCsj47335	Failure to deploy a Route, GTT, or Address table file to the *slot:* or *bootflash:* on an ITP 7200 or 7300. The exception contains the text "Verifying checksum."
CSCsj03709	Link Q.752 measurements were missing from the MWTM web interface. The following tabs were added to the web: Linkset > Statistics, Link > Statistics, Link > Q.752 Measurements, Link > SCTP Assoc. Config Details, Link > SCTP Assoc. Stats Details, Link > Interface Details.
CSCsj11353	The RAN Shorthauls column is missing in the web summary lists table.
CSCsi65863	Enhanced command to collect data within date range. See mwtm collectstats, page 16.
CSCsk21900	New **mwtm iosreport** command for reporting node name, display name, node type, IOS version, and serial number in CSV format. See mwtm iosreport, page 17.
CSCsj77053	Added alarmsummary keyword to the mwtm print command. See mwtm print, page 17.
CSCsk38892	SNMP trap rate limiting feature for alarms and events.
CSCsl26972	Added new commands to modify the trap rate count and interval. See mwtm trapratelimit, page 18.

Bug ID	Description
CSCsj75651	Improve the CLI for setting TFTP parameters in these MWTM commands: gttdir, routedir, and atbldir. See Improved Command Prompting, page 20.
CSCsj55259 CSCsj64394 CSCsj18583 CSCsj76386 CSCsj76388 CSCsj76395 CSCsk52393	Added support for the ASN Gateway personality, discovery, events, alarms, real-time pollers, real-time tabs, troubleshooting commands, and syslog messages.
CSCsi23881 CSCsj76398	Added fault support and PWE3 show commands in the MWTM Troubleshooting tab.
CSCsh61570	ITP: Loading address table launches file management for full flash.
CSCsk27006	Replace native OS Telnet terminal with MWTM terminal. Users can still continue to launch external Telnet programs by setting these preferences in the MWTM.
CSCsj46171 CSCsk19684 CSCsj40633	Discovery, web launch, and fault support for Cisco Database for Telecommunications (CDT) 2.0 (number portability for ITP).
CSCsg88828	Change RAN-O to CSR (Cell Site Router) in the Credentials tab.
CSCsb71174 CSCsj74649	Provide real-time statistics for CPU and memory utilization in the MWTM client and web interfaces. See CPU and Memory Utilization Statistics, page 5.
CSCsk33564 CSCsj74663 CSCsh12862 CSCsj74616 CSCsk45059 CSCsk32285 CSCsj74633	Support for MIB II interface statistics (Interface Performance and Interface Errors tabs in the MWTM Java and web clients, poller, traps). See Viewing Real-Time Data for Interfaces, page 7.
CSCsk15849	Virtual backhaul historical data is not updated if report polling is disabled on the nodes that have backhauls belonging to the virtual backhaul.
CSCsk25646	Updated disk size recommendation to 60GB. Updated swap size to equal the RAM size. Replaced SunFire V210 recommendation with SunFire V215 or V245.
CSCsj86420 CSCsj86438 CSCsj86440 CSCsj74676 CSCsj74692 CSCsl01340	Support for TDM drop and insert real-time statistics, fault support, troubleshooting commands, traps, and alarms.
CSCsi67179 CSCsi65636 CSCsk42790 CSCsj36705 CSCsi65629 CSCsk42788	Support for enhanced HA on the MWTM (traps, alarms, personality type, troubleshooting).
CSCsj93819	In the navigation tree, changed Alarms to Active Alarms and Events to Event History.

Bug ID	Description
CSCsh98358 CSCsh98352 CSCsh98345 CSCsh98349 CSCsh90827 CSCsc91157 CSCsh90827	MWTM support for CSG1, CSG2, GGSN 6 and 7, and generic nodes.
CSCsj76347 CSCsj76359 CSCsj76367 CSCsj76372	Support for CSG2 (Statistics tab, troubleshooting, poller, traps, and alarms).
CSCsk21891	Distinguish between CSG1 and CSG2 devices in the MWTM GUI.
CSCsl04496	Change default message log size from 50,000 to 500,000 messages in the *System.properties* file.
CSCsk48622 CSCsk48575 CSCsk48619 CSCsk48569 CSCsj93812 CSCsk48628 CSCsk48637 CSCsk48668	Changed alarm style to ITU X.733 Style (topology, Java GUI tabs, Java navigation tree, web GUI changes, events, traps, upgrade).
CSCsk27672 CSCsj93897	Added Active Alarm Summary List to MWTM Java and web client interfaces.
CSCsk70976 CSCsk70974 CSCsk70967	Added event queue status icon to MWTM Java and web client interfaces to indicate when event queue threshold has been exceeded.
CSCsk50370	Ad-hoc user queries can cause java.lang.outOfMemory error on server.
CSCsl17412	Remove Severities item from event editor left pane.
CSCsl06517	Distinguish peer events and alarms in subtabs under Recent Events and Alarms tabs.
CSCsj43020	Add support for the MWTM Linux server and MWTM Linux Client to run on CentOS the same way that they run on RedHat 4.
CSCsj56816	• Expanded ITP event help pages with troubleshooting guidance • Included troubleshooting commands for ITP • Created a separate category for ITP and moved ITP commands to this category
CSCsk70707 CSCsk70710	Third-party integration launch capability from MWTM Tools menu.
CSCsl26972	Introduce **mwtm trapratelimit** command to modify trap rate limiting count and interval.
CSCsl48565	Separate Readme and MIB listings on the MWTM web interface for the ASN Gateway and HA.
CSCsj02446 CSCsj23958	MWTM and CiscoWorks integration.
CSCsi94803	MWTM discovery does not handle network and broadcast address.

Bug ID	Description
CSCsb36783	MWTM Client: Navigate to filtered events when clicking the event icon.
CSCse11825	MWTM Client: Main window should support a horizontal scroll bar.
CSCse66578	Added MWTM support for MWR modules NM-1A-OC3SMI, NM-1A-T3, and NM-16ESW configured with GSM and UMTS.
CSCsg47612	ITP: Reflect MSU rate threshold levels in the node status information.
CSCsh38411	MWTM web client: Refresh interval should not revert back to selected value when navigating to a new page.
CSCsh89544	Exception in virtual linkset processing.
CSCsi26122	Use last updated timestamp after removal of note instead of reverting to *Not Set*.
CSCsi52328	The validateSystem.sh file reports too many processors on some Linux servers.
CSCsi91340	Password age message appears even if aging is not set.
CSCsi96549	Alarm display issues with alarm filtering based on device selection.
CSCsj14797	User login occurs when a change-password operation fails.
CSCsj14839	Default icon for legacy RAN-O objects incorrectly appears as an IP device.
CSCsj18336	Error occurs when deleting over 100 events in the web client.
CSCsj20029	Remove unused variable USE_TERMINAL_PROXY from client properties.
CSCsj45690	Performance graph shows wrong time zone information.
CSCsj46186	MWTM client: Improve foreground text colors in event and alarm tables.
CSCsj46191	Allow immediate archival of cleared alarms.
CSCsj47348	The **mwtm listarchive** command output needs improvement.
CSCsj60998	MWTM fails to determine backhaul peer if one shorthaul is down.
CSCsj66339	OSS Integration Guide is not in the build.
CSCsj70382	Deployment of file to slot0 produces an error message.
CSCsj73141	Application server could be polled with no routing key defined.
CSCsj76863	MWTM client: Improve graph line colors.
CSCsj94701	ASN-GW and CSG2: Launch web advanced details tab,
CSCsj97482	Include CSG Service Manager 4.1.3 and GGSN Service Manager 4.1.3 as installation options in MWTM 6.0.2.
CSCsk07359	RAN shorthauls column always contains zeros in Summary Lists table.
CSCsk43296	Launching MWTM home page fails from CiscoWorks dashboard when SSL is enabled on CiscoWorks but not on MWTM server.
CSCsk50978	MWTM and Service Manager links do not properly appear on CiscoWorks dashboard.
CSCsk52579	Added new user preferences in the web client preferences pane.
CSCsk65727	User cannot cancel **mwtm servername** command.
CSCsk88995	Error message can occur if user runs **mwtm status** command but server is not started.
CSCsl13284	Support new GTT file format 4.4 version in MWTM.
CSCsk15913	Third-party integration with web Details tabs.
CSCsk15921	(Integration) Advanced drill-down tab pane options.

Bug ID	Description
CSCsk25827	Improve discovery performance for large MWR networks.
CSCsl28045	Delete all alarms during a discovery with purge.
CSCsl83044	Some MWTM commands do not work when SSL is enabled.

Open MWTM Caveats

This section describes caveats that exist in the MWTM 6.0.2 software.

- CSCse81393

Symptom In various GUI and web pages, simple text fields might contain unprintable characters. An example is the Model Name PID field for a RAN service (RAN_SVC) card in an ONS chassis.

Conditions Some RAN_SVC cards in an ONS chassis can exhibit this behavior.

Workaround None. This is a cosmetic problem and does not affect functionality.

- CSCsg83861

Symptom The preferences dialog box of the MWTM client interface allows you to customize the way that data series appear in charts. You can specify series color, line style, and symbol style. However, symbol style and line style preferences do not work when displaying real-time charts for MSU rates and for RAN backhauls and shorthauls.

Workaround None.

- CSCsg92892

Symptom When provisioning ITP nodes from the Provision tab of the web interface, some provisioning operations might fail on the node with these symptoms and conditions:

Provisioning Action	Symptom	Condition
Changing the media type for FastEthernet or GigabitEthernet interface	`Invalid input detected`	FastEthernet or GigabitEthernet on the node does not support the media type configuration option, but the user specified a media type in the MWTM provisioning request.
Changing speed for FastEthernet or GigabitEthernet interface	`Invalid input detected`	FastEthernet or GigabitEthernet on the node does not support the speed configuration option, but the user specified the speed in the MWTM provisioning request.
Configuring MTP3 User Adaptation (M3UA) or SCCP User Adaptation (SUA) offload, or Local Peer offload	`Error: at least one address must reside on slot xx`	The user specified an IP address that does not exist for the specified card slot.
Configuring M3UA or SUA offload, or Local Peer offload	`Error: XXX is already offloaded to this linecard slot=xx`	The user specified a target card slot that is already in use by another M3UA or SUA offload, or Local Peer offload. **Note** The ITP does not allow mixed types between M3UA or SUA offload, and Local Peer offload.
Configuring the line priority for the clock source line option on the Cisco 2600 T1/E1 controller	`% Invalid input detected at '^' marker.` The '^' marker points to the line priority: *primary* or *secondary*.	While configuring the clock source line priority option on the T1/E1 controller, the user specified the *primary* or *secondary* option on the line, but the WAN Interface Card (WIC) card has only one port, and does not support the line priority option.
Configuring the secondary line priority for the clock source line option on the Cisco 7xxx ITP T1/E1 controller	`% Invalid input detected at '^' marker.` The '^' marker points to the secondary line priority: *primary* or *secondary*.	When configuring the clock source secondary line priority option on the T1/E1 controller, the user specified a number that is greater than the supported range on the device. Although the MWTM allows values 1–72, some cards only support 1–8 or 1–16.

Workaround None. The user must know the ITP card information and specify correct values in the provisioning request.

- CSCsh00145

Symptom Credentials for a node are associated with a unique IP address. If a node has more than one accessible IP address, functions that require credentials might not resolve to a credential based on the selected IP address, and the requested function would fail. The MWTM functions that require credentials include:

- Discovery of ONS and RAN_SVC nodes
- Troubleshooting
- Provisioning
- Route and Global Title Translation (GTT) table deployment

Conditions Nodes with multiple, accessible IP addresses with credentials set for a subset of those IP addresses.

Workaround Specify credentials for all accessible IP addresses for a node.

- CSCsh15638

Symptom The following exception with corresponding stacktrace can occur. The MWTM captures this exception in the *sgmConsoleLog.txt* file*:*

```
java.net.SocketException: Broken pipe
```

Conditions This exception can occur when users access the MWTM web interface and frequently abort connections while the server is under heavy load (for example, during discovery). Clicking the **Stop** button on the web browser or navigating to a different web page before the current page finishes loading can cause this exception to occur.

> **Note** The root cause of this condition is an internal bug in the Tomcat web application that ships with this release of the MWTM.

Workaround None, but you can safely ignore these log messages.

- CSCsh58070

Symptom The following error messages may appear when performing these operations:

Operation	Error Message
Generating link report by using the *sgmLinkStats.sh* script	`sgmgawk: cmd. line:45: (FILENAME=- FNR=???)` `fatal: division by zero`

Attempting to import link and linkset report data	`ERROR 38000: The exception`
	`'java.sql.SQLException: Invalid character`
	`string format for type SMALLINT.' was thrown`
	`while evaluating an expression.`

Using the ITP route table deployment function	`Invalid Linkset in Route Table: [???]`

Conditions The error messages occur when ITP linkset, AS, and ASP names contain a colon (:).

Workaround Remove the colon (:) from ITP linkset, AS, and ASP names.

- CSCsi68842

Symptom Negative numbers appear in the Error counts table for RAN shorthauls and backhauls.

Workaround None.

- CSCsl57558

Symptom After starting the 6.0.1 Java client, an error dialog displays a target invocation error. Click OK, and the client displays a blank, white screen on the right side.

Conditions The event window was customized in 6.0 and the 6.0.1 patch is applied.

Workaround Follow these steps:

1. Shut down the MWTM server.
2. Remove the */opt/CSCOsgm/prefs/.java* directory.
3. Restart the server and the client starts correctly.

You can also work around this problem by applying the 6.0.2 (or later) patch (because the upgrade procedure removes client preferences).

- CSCsl68270

Symptom The MWTM incorrectly deploys a version 4.4 GTT file to a node running an IOS image that does not support GTT 4.4. You cannot reload the version 4.4 file in the GTT editor after deploying it.

Workaround Deploy GTT 4.4 files only to nodes that are running these supported IOS images: 12.2(18)IXE+ and 12.4(15)SW+.

- CSCsm05182

Symptom A node object in the navigation tree appears with an alarm severity other than normal when there are no alarms associated with the node.

Conditions The node was originally discovered with an invalid community string and subsequently rediscovered with a correct community string.

Workaround Set the node to unmanaged action; then set the node to managed. Restarting the MWTM server will also correct the problem.

Open Device Caveats

This section documents caveats associated with the devices that the MWTM manages. These caveats can affect the capability of the MWTM to manage the associated features. Follow the guidelines in the workarounds for these defects.

- CSCse13374

Symptom When you configure the clock source on an ITP 7600 IMA interface to a nondefault value, if the ITP 7600 reboots, the clock source reverts to the default value, "line".

Workaround Reapply the clock source on all the IMA interfaces after the ITP 7600 reboots.

- CSCsg76526

Symptom When you unconfigure Preventive Cyclic Retransmission (PCR) from an MTP2 link on an ITP device, the device incorrectly retains tuning parameters, such as *n1* and *n2*, in the running configuration.

Conditions You configure PCR and set tuning parameters with values other than default values.

Workaround Unconfigure the tuned parameter first. Then, unconfigure PCR.

- CSCsg77134

Symptom When you unconfigure a tuned parameter for a link that belongs to a linkset with a configured profile, the default value for the timer is incorrectly restored instead of the profile timer value.

Conditions The cs7 profile is overriding the profile value.

Workaround Unconfigure and reconfigure the profile for the linkset. This action should restore the profile value to all links.

- CSCsg77152

Symptom When you configure the following parameter for an SCTP link:

```
retransmit-cwnd-rate <rate> sctp-fast-retransmit
```

the *sctp-fast-retransmit* portion is not saved in the configuration, and is ignored at the next reload.

Conditions Tune the *sctp-fast-retransmit* parameter for *retransmit-cwnd-rate*.

Workaround Reconfigure the parameter after reloading the device.

- CSCsh13017

Symptom The MWTM login credentials might not work if you run the **no enable secret** command on the active RAN Service (RAN SVC) Module.

Conditions During failover, the running configuration on the active RAN service card merges with the RAN protection card. As a result, any baseline configuration command that exists on the protection card but not on the active card will be applied.

Workaround For all RAN service cards:

- Apply the enable-secret configuration option.
- Define these credentials in the MWTM.

Related Documentation

Use this document in conjunction with the following documents:

- *Installation Guide for the Cisco Mobile Wireless Transport Manager 6.0*
- *User Guide for the Cisco Mobile Wireless Transport Manager 6.0*
- *OSS Integration Guide for the Cisco Mobile Wireless Transport Manager 6.0*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.