APPENDIX C

FAQs

This appendix contains:

General FAQs

These categories of frequently asked questions are general questions about the Cisco Mobile Wireless Transport Manager (MWTM):

Installation Questions

This section addresses the following installation questions:

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:

Step 1 Delete the MWTM client installation directory and its contents. If you installed the MWTM client in the default directory, *C:\Program Files*, then the installation directory is *C:\Program Files\Cisco Systems\MWTM Client*. If you installed the MWTM client in a different directory, then the installation directory resides in that directory.

Step 2 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?

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?

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?

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?

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?

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/CSCOsgm/bin/mwtm useraccess disable

Output similar to the following appears:

```
[root@mwtm-server bin]# /opt/CSCOsgm/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/CSCOsgm/bin/mwtm useraccess enable

Step 3 Run the following command:

/opt/CSCOsgm/bin/mwtm adduser <username>

Output similar to the following appears:

```
[root@mwtm-server bin]# /opt/CSCOsgm/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/CSCOsgm/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?

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	• 12.2 (18) IXB or later • 12.2 (25) SW7 or later • 12.4 (11) SW or later
MLR Details	All	• 12.2(18)IXA or later • 12.2(21)SW1 or later • 12.4(11)SW or later
Non-Stop Operation	Cisco 7500 and Cisco 7600 nodes only	• 12.2 (18) IXA or later • 12.2(21)SW or later • 12.2 (4)MB13a or later

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?

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[1]	Generated
Trap polling	Traps do not trigger polling	Traps do trigger polling
Regular polling[2]	Performed	Performed
Real-time polling	Available[3]	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

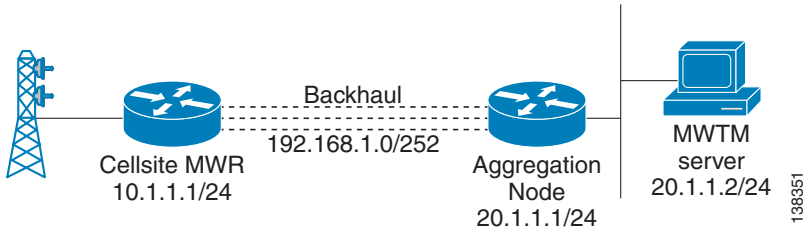
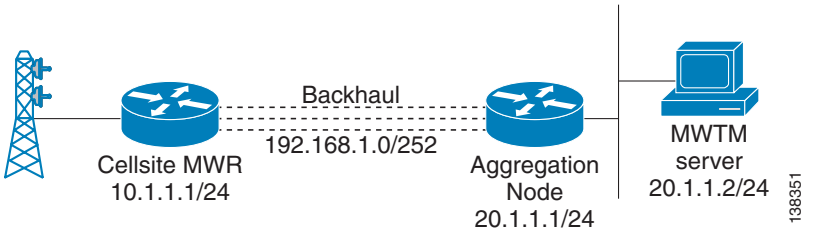


Figure C-2 Example of Static Routing



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:

a. Stop the NTP software using the following command:

```
/etc/init.d/ntpd 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 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/ntpservers*) 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/ntpd 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.