Release Notes for the Cisco Mobile Wireless Transport Manager 6.0

Date: March 8, 2007

These release notes describe the caveats for the Cisco Mobile Wireless Transport Manager (MWTM), Release 6.0. 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:

- Introduction, page 2
- What's New in MWTM 6.0, page 2
- Limitations and Restrictions, page 3
- Open MWTM Caveats, page 4
- Open Device Caveats, page 8
- Related Documentation, page 10
- Obtaining Documentation, page 10
- Documentation Feedback, page 11
- Cisco Product Security Overview, page 11

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

- Obtaining Technical Assistance, page 12
- Obtaining Additional Publications and Information, page 14

Introduction

These release notes describe caveats, known bugs, and other important information for installing and using MWTM 6.0.

What's New in MWTM 6.0

The MWTM 6.0 release provides an upgrade path for existing users of the:

- Signaling Gateway Manager (SGM) 4.1
- Mobile Wireless Transport Manager (MWTM) 5.0

The MWTM 6.0 release provides these new features:

What's New for SGM 4.1 Users	What's New for MWTM 5.0 Users
Integration of Northbound Application Programming Interface (API), Operations Support System (OSS)	Integration of northbound API, OSS
Alarm correlation	Alarm correlation
Enhanced web interface	Enhanced web interface
Improved web-based reporting features	Improved web-based reporting features
Support for Secure Shell (SSH) communication between server and nodes	Support for SSH communication between server and nodes
Server support for Red Hat Enterprise Linux (RHEL) Advanced Server (AS) 4.0	Server support for RHEL AS 4.0
Server support for Solaris 10	Server support for Solaris 10
Data stored in relational database	Data stored in Relational Database
Wizard-based provisioning of links, linksets, application servers (AS), and application server processes (ASP)	Support for Cisco Optical Networking System (ONS) 15454 and ONS-based RAN Service (RAN SVC) Module
Integration of northbound API, OSS for provisioning of links, linksets, AS, and ASP	Troubleshooting tools
Support for Message Signal Unit (MSU) rates	Enhanced RAN backhaul and shorthaul performance graphs
Support for Cisco 2811 and IOS 12.4 SW	—

For a detailed list of features that the MWTM 6.0 release provides, see the "Overview" chapter of the *User Guide for the Cisco Mobile Wireless Transport Manager 6.0*.

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.

MWTM Telnet Proxy

If you enable the MWTM Telnet proxy (**mwtm tnproxy enable** command), you cannot use an external Telnet program to connect to a node from the MWTM client; you must use the Telnet program that comes with the MWTM.

To use an external Telnet program, you must disable the MWTM Telnet proxy (**mwtm tnproxy disable** command).

Open MWTM Caveats

This section describes caveats that exist in the MWTM 6.0 software:

- CSCsc88099

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 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.

- CSCsg83861

Symptom The preferences dialog 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

- 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.

- 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.

- 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). Pressing 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 avoid 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.

- 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 provision 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.

- CSCef67144

Symptom Sometimes when using the client on a Solaris multi-processor computer, an exception occurs when the topology window is open and you are manipulating views.

Workaround Close the topology window, then reopen it.

- CSCsg62928

Symptom The RAN-O backhaul performance charts can show incorrect % Utilization (Y axis, on the right side of the chart).

Conditions RAN-O backhaul interfaces with asymmetric link speeds or different physical interfaces for send and receive traffic. For example, you might observe this symptom if the backhaul uses Digital Subscriber Line (DSL) or cable media.

Workaround Use the Y axis on the left side of the chart, which shows backhaul utilization in bits or bytes per second.

- CSCsh89439

Symptom Loading the GTT table from an ITP might fail with this error message:

```
nameFormatErr
```

Conditions The ITP network name contains a space ( ) character.

Workaround Remove the space ( ) character from the ITP network name, or use an underscore (_) or a hyphen (-) instead of the space ( ).

- CSCsh89933

Symptom When you select a shorthaul in the navigation tree of the MWTM web interface, and click the Errors tab, the total number of errors displayed might not equal the sum of the individual errors because of rounding errors. The total number of errors might be one or two counts more or less than the sum of the individual errors.

Conditions You have enabled RAN-O statistics collection.

Workaround None. These minor mismatches will cancel each other over a few adjacent report intervals. The mismatches do not accumulate over a period of time.

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.

- 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.

- CSCsh71843

Symptom The Management Information Base (MIB) ifTable does not contain T1/E1 controllers for the T1/E1 controllers on the Cisco 2600 WIC card.

Conditions The Cisco 2600 with a T1 or E1 WIC card running IOS 12.4(11)SW.

Workaround None. You cannot use the MWTM to:

- Show T1/E1 controllers on the Cisco 2600 running IOS 12.4(11)SW.
- Provision T1/E1 controllers or channelized serial interfaces on the Cisco 2600 running IOS 12.4(11)SW.

- 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

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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