



Release Notes for GGSN 5.0 on the Catalyst 6000 / Cisco 7600 MWAM for Cisco IOS Software Release 12.3(8)XU4

December 20, 2004

Cisco IOS Release 12.3(8)XU4

OL-5266-08

These release notes for the Cisco GGSN Release 5.0 on the Cisco Multi-processor WAN Application Module (MWAM) describe the enhancements provided in Cisco IOS Release 12.3(8)XU4. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(8)XU4, see the “[Caveats in Cisco IOS Release 12.3\(8\)XU4](#)” section on page 6 and *Caveats for Cisco IOS Release 12.3 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.3* located on Cisco.com and the Documentation CD-ROM.

Documentation Survey

Is Cisco documentation helpful? Click [here](#) to give us your feedback or go to the following URL to give us your feedback:

<http://forums.cisco.com/eforum/servlet/viewsflash?cmd=showform&pollid=rtgdoc01!rtgdoc> to give us your feedback .

Contents

These release notes describe the following topics:

- [Introduction to Cisco GGSN on the Cisco MWAM, page 2](#)
- [System Requirements, page 3](#)



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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

- [Related Documentation, page 12](#)
- [Limitations, Restrictions, and Important Notes, page 5](#)
- [New and Changed Information, page 5](#)
- [Caveats in Cisco IOS Release 12.3\(8\)XU4, page 6](#)
- [Cisco MWAM Caveats with Cisco IOS Release 12.3\(8\)XU4, page 10](#)
- [Related Documentation, page 12](#)
- [Documentation Roadmap for Implementing GGSN Release 5.0 on the Cisco MWAM, page 14](#)
- [Obtaining Documentation, page 15](#)
- [Documentation Feedback, page 16](#)
- [Obtaining Technical Assistance, page 16](#)
- [Obtaining Additional Publications and Information, page 17](#)

Introduction to Cisco GGSN on the Cisco MWAM

The following sections describe Cisco GGSN and the Catalyst 6500 / Cisco 7600 Multi-processor WAN Application Module (MWAM).

- [Cisco GGSN Overview, page 2](#)
- [Cisco MWAM Overview, page 3](#)

Cisco GGSN Overview

Gateway GPRS support node (GGSN) is a service designed for Global System for Mobile Communications (GSM) networks. GSM is a digital cellular technology that is used worldwide, predominantly in Europe and Asia. GSM is the world's leading standard in digital wireless communications.

The general packet radio service GPRS is standardized by the European Telecommunications Standards Institute (ETSI). The most common application of GPRS is expected to be Internet/intranet access. Cisco Systems' GPRS solution enables mobile wireless service providers to supply their mobile subscribers with packet-based data services in GSM networks.

GPRS introduces the following two new major network elements:

- **SGSN**—Sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The Serving GPRS Support Node (SGSN) communicates between the mobile station (MS) and the GGSN. SGSN support is available from Cisco partners or other vendors.
- **GGSN**—A wireless gateway that allows mobile cell phone users to access the public data network (PDN) or specified private IP networks. The GGSN function is implemented on the Cisco Systems' router.

Cisco GGSN Release 5.0 provides combined 2.5G and 3G packet gateway support and interworking capability on the same node.

Cisco MWAM Overview

With Cisco IOS Software Release 12.3(2)XB and later, the Cisco GGSN software can run on the Cisco MWAM installed in a Catalyst 6500 series switch or Cisco 7600 series router.

The MWAM provides three processor complexes with dual processors used in two of the complexes and a single processor used in the remaining processor complex. This architecture provides five mobile wireless applications on one module.

The MWAM does not provide external ports but is connected to the switch fabric in the Catalyst 6500/Cisco 7600 chassis. An internal Gigabit Ethernet port provides an interface between each processor complex and the Supervisor module. Virtual Local Area Networks (VLANs) direct traffic from external ports via the Supervisor module to each mobile wireless application instance.

The MWAM provides an interface to the IOS image on the Supervisor module. The Supervisor module software enables a single session to be established to each application on the MWAM(s) in the chassis. Each session is used for configuring, monitoring, and troubleshooting application. For information on establishing sessions to mobile wireless application instances on the MWAM, refer to the [Cisco Multi-Processor WAN Application Module Installation and Configuration Notes](#):

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/mwam_1cn.htm



Note

In this release, each application on the MWAM must be configured individually.

The software image that provides the mobile wireless application feature is downloaded through the Supervisor module and distributed to each processor complex on the MWAM(s). The same image is installed on all the processors in the MWAM.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(8)XU4 and includes the following sections:

- [Memory Recommendations, page 3](#)
- [Hardware and Software Requirements, page 4](#)
- [Determining the Software Version, page 4](#)
- [Upgrading to a New Software Release, page 4](#)

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.3(8)XU1

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MWAM on Catalyst 6500 / Cisco 7600 MWAM	GGSN Standard Feature Set	c6svc-mwam-g8is-mz.b1.123-8.XU4.bin	48MB	512MB	RAM

Hardware and Software Requirements

Cisco IOS Release 12.3(8)XU4 requires the following hardware and software:

- Cisco MWAM
- Catalyst 6500 series switch / Cisco 7609 series router
- Supervisor Engine 2 module with the Multilayer Switch Feature Card (MSFC2) card on which Cisco IOS Release 12.2(17d)SXB1 or later is installed.

For information about Cisco IOS Release 12.2(17d)SXB1, refer to the documentation on Cisco IOS Release 12.2 SX New Features available at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/index.htm>



Note

A Hardware-Software Compatibility Matrix is available on CCO for users with CCO login accounts. This matrix allows users to search for supported hardware components by entering a Cisco platform and IOS Release. The Hardware-Software Compatibility Matrix tool is available at the following URL:

<http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hswmatrix.cgi>

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco MWAM, log in to the router on one of the MWAM processors and enter the **show version EXEC** command:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) MWAM Software (MWAM-G4JS-M), Version 12.3(8)XU4, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
```

Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Upgrade Ordering Instructions* located at:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

Upgrading IOS Image on MWAM

For information on upgrading IOS images on the MWAM, refer to the *Cisco Multi-Processor WAN Application Module Installation and Configuration Notes*:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/mwam_icn.htm



Note

The image download process loads the IOS image onto the three processor complexes on the MWAM.

Upgrading ROMMON Software

To perform an ROMMON software upgrade, use the procedure provided in the *Cisco Multi-Processor WAN Application Module Installation and Configuration Notes*.

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Limitations, Restrictions, and Important Notes

When using Cisco IOS Release 12.3(8)XU, observe the following:

- Only five instances of the Cisco IOS Release 12.3(8)XU4 image can be loaded onto the MWAM.
- The same Cisco IOS image must be loaded onto all processor complexes on the MWAM.
- Session console is provided by a Transmission Control Protocol (TCP) connection from the Supervisor module (no direct console).
- Available memory for bootflash for saving crash information files is 500 KB.
- Only five files can be stored in the bootflash filesystem.
- VPN routing/forwarding (VRF) instances are not supported on the Catalyst 6500 / Cisco 7600 Supervisor/MSFC2, therefore, you must tunnel encapsulated VRF traffic through the Supervisor/MSFC2 via a generic routing encapsulation (GRE) tunnel. For more information, see the *Cisco GGSN Release 5.0 Configuration Guide*.

New and Changed Information

The following section lists the new implementations and behavior changes in the Cisco IOS Release 12.3 XU releases:

- [New Features in Cisco IOS Release 12.3\(8\)XU4, page 5](#)
- [New Features in Cisco IOS Release 12.3\(8\)XU3, page 5](#)
- [New Features in Cisco IOS Release 12.3\(8\)XU2, page 6](#)
- [New Features in Cisco IOS Release 12.3\(8\)XU1, page 6](#)
- [New Features in Cisco IOS Release 12.3\(8\)XU, page 6](#)

New Features in Cisco IOS Release 12.3(8)XU4

There are no new features supported by the Cisco MWAM on the Catalyst 6500 / Cisco 7600 platform for Cisco IOS Release 12.3(8)XU4.

New Features in Cisco IOS Release 12.3(8)XU3

There are no new features supported by the Cisco MWAM on the Catalyst 6500 / Cisco 7600 platform for Cisco IOS Release 12.3(8)XU3.

New Features in Cisco IOS Release 12.3(8)XU2

There are no new features supported by the Cisco MWAM on the Catalyst 6500 / Cisco 7600 platform for Cisco IOS Release 12.3(8)XU2.

New Features in Cisco IOS Release 12.3(8)XU1

There are no new features in Cisco IOS Release 12.3(8)XU1.

New Features in Cisco IOS Release 12.3(8)XU

The following new features are supported in Cisco IOS Release 12.3(2)XU:

- Quality of Service (QoS)
 - Call Admission Control (CAC)
 - Per-packet data protocol (PDP) policing
- Charging
 - Time trigger
 - Charging profiles
 - Tertiary charging gateway
 - Switchback to primary charging gateway
- Maintenance mode
- Multiple access point names (APNs) per VRF
- Multiple trusted public land mobile network (PLMN) IDs
- GGSN-IOS server load balancing (SLB) messaging
- Session timeout

For information on each of these features see the Cisco GGSN Release 5.0 configuration guide and command reference:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xu/index.htm>

Caveats in Cisco IOS Release 12.3(8)XU4

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T are also in Cisco IOS Release 12.3(8)XU4.

For information on caveats in Cisco IOS Release 12.3, see *Caveats for Cisco IOS Release 12.3*.

For information on caveats in Cisco IOS Release 12.3 T, see *Caveats for Cisco IOS Release 12.3T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

Using the Bug Navigator II

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats the most current list of caveats of any severity for any software release. To reach Bug Navigator II, Login to Cisco.com and click **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go directly to <http://www.cisco.com/support/bugtools>.

Open Caveats

This section documents possible unexpected behavior by Cisco IOS Release 12.3(8)XU4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee79534

Description: When a Cisco MWAM GGSN IO memory becomes very low, it might not be possible to session to the GGSN (processor) from the Catalyst 6500 / Cisco 7600 supervisor module.

Workaround: There is currently no known workaround.

- CSCee87603

Description: When a DHCP server is not able to renew all requests from a GGSN, a memory allocation failure occurs when the GGSN tried to delete PDPs, resulting in a traceback.

Workaround: There is currently no known workaround.

- CSCee88746

Description: The Cisco GGSN displays a **gprs charging cdr-option sgsn-plmn** configuration in the show running configuration even though the command is no longer configured. This condition exists when the **gprs charging cdr-option sgsn-plmn** command is configured and GGSN services are disabled and then re-enable on the router using the **[no] service gprs ggsn** command.

Workaround: Disable the **gprs charging cdr-option sgsn-plmn** command configuration before disabling GGSN services.

- CSCee94797

Description: A Cisco router running the Cisco GGSN Release 5.0 software increments both the Optional IE Invalid and Optional IE Incorrect counters. This condition occurs when the protocol configuration option (PCO) in the Create PDP Context request contains two Challenge Handshake Authentication Protocol (CHAP) messages that both have different usernames and a code of "Response".

Workaround: There is currently no known workaround.

- CSCef29307

Description: When the charging functionality is under a lot of stress and the charging gateway is going up and down frequently, causing a high volume of charging data records being queued, the Cisco GGSN does not clear the TCP socket from the GGSN to the charging gateway and therefore, does not respond to the nodealive requests from the charging gateway.

Workaround: Display the Transmission Control Block (TCB) address of the connection to clear by issuing the **show tcp brief** command. Clear the connection by issuing the **clear tcp tcb** command and specifying the TCB address obtained from the **show tcp brief** command and then send a nodealive from the charging gateway.

- CSCef30823

Description: A Cisco router running Cisco GGSN Release 5.0 rejects duplicate GPRS Tunneling Protocol Version 1 (GTPv1) primary PDP contexts containing traffic flow template (TFT) information when the **gprs gtp create-request v1 update-existing-pdp** command is enabled.

Workaround: There is currently no known workaround.
- CSCef31241

Description: The Cisco GGSN often adds one extra byte before the LRSN value and converts the LRSN into a 5-byte value. According to Third Generation Partnership Program (3GPP) standard 32.2.15, the LRSN number should be an unsigned integer of four octets.

Workaround: There is currently no known workaround.
- CSCef32820

Description: The Cisco GGSN deletes an existing GTPv0 PDP context and recreates it when a new Create PDP Context request with a different restart counter for the existing PDP context is received from a different SGSN. This condition occurs only if existing PDP contexts on the path to the second SGSN already exist and have a different restart counter than the new Create PDP Context request. The GGSN should delete the PDPs on the path of the second SGSN and process the second Create PDP Context request as an Update PDP Context request.

Workaround: There is currently no known workaround.
- CSCef44957

Description: The data_msg_dropped counter, displayed by the **show gprs gtp statistics** command, is not incremented when an invalid IP packet is received.

Workaround: There is currently no known workaround.
- CSCeg01375

Description: The creation time of a PDP context displayed using the **show gprs gtp pdp tid** command might vary when the command is executed multiple times. This condition does not affect charging-related functions for the PDP context.

Workaround: There is currently no known workaround.
- CSCin74608

Description: The Cisco GGSN might reload due to memory corruption.

Workaround: There is currently no known workaround.
- CSCin76672

Description: On a Cisco GGSN, for a PPP type PDP context for which the PPP session endpoint is on the GGSN, if the MS deletes the PPP session by sending “LCP TERMREQ,” the cause code used by the GGSN in the associated call detail record (CDR) is “abnormalRelease.” If the MS initiates the closing by sending a GTP delete PDP context request to the GGSN, this condition does not occur (the cause code used in the CDR is “normalRelease”).

Workaround: There is currently no known workaround.

Resolved or Closed Caveats

The caveats listed in this section are resolved or closed in Cisco IOS Release 12.3(8)XU4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw08251

Description: When RADIUS servers are down and an APN requested by a user is in non-transparent mode, the cause value in the create PDP request response failure is incorrect.

- CSCee22639

Description: When the **ip tcp adjust-mss** command is configured on a Cisco router and there is IP fragmentation, data corruption might occur on some IP fragments. The corruption is not detected by the TCP checksum utility.

- CSCee36192

Description: After configuring the **no snmp-server enable traps tty** command and issuing a **write mem**, the **snmp-server enable traps tty** configuration is present in the running config but

- CSCee67450

A Cisco device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command 'bgp log-neighbor-changes' configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

If a malformed packet is received and queued up on the interface, this bug may also be triggered by other means which are not considered remotely exploitable such as the use of the command 'show ip bgp neighbors' or running the command 'debug ip bgp <neighbor> updates' for a configured bgp neighbor.

Cisco has made free software available to address this problem.

For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

- CSCef19117

Description: A Cisco router on which the **ip tcp adjust-mss** command has been configured might fail to set the value for outbound packets.

- CSCef75301

Description: When a create PDP context request contains more than 13 octets of QoS profile, the Cisco GGSN does not accept the profile.

- CSCeg08927

Description: A Cisco router running Cisco GGSN software reloads in some cases that involve repetitive create PDP context requests on an existing PDP.

- CSCeg18250

Description: A Cisco router running Cisco GGSN software reloads when a peer device sends data packets into the control path.

- CSCeg35627

Description: Upon receiving a create request from a WAP gateway when anonymous access is configured for an access-point, the Cisco GGSN does not send username as MSISDN.

- CSCeg41118
Description: A Cisco router running Cisco GGSN software reloads if an incorrect GTP Version 1 (GTPv1) delete PDP context request is received with the Tunnel Endpoint Identifier (TEID) set to Data TEID assigned by the GGSN instead of Control TEID.
- CSCin85534
Description: When the “apnUnreachable,” “authenticationFail,” “ipAllocationFail,” and “noResource” failure conditions occur on the GGSN, the GGSN sends a notification. Since these failure conditions occur during the activation of a PDP context, the traps directly depend on the context activation rate and therefore cause flooding.

Cisco MWAM Caveats with Cisco IOS Release 12.3(8)XU4

This section lists the Cisco MWAM caveats that are open and resolved with Cisco IOS Release 12.3(8)XU4.

Open Caveats

The following Cisco MWAM caveats open with Cisco IOS Release 12.3(8)XU4.

- CSCee30049
Description: A spoofed KMP heartbeat message received by a Cisco MWAM processor from an external packet generator via switch-fabric or system-bus might cause alignment errors. This is not a real-life scenario (the heartbeat messages should be coming from the PC via EOBC actually), so this may not be a serious concern.
Workaround: There is currently no known workaround.
- CSCee36284
Description: If a Cisco MWAM is under heavy traffic load, and a reset is issued, the MWAM might reload twice. This causes an increased reload time. A crashinfo file is also generated.
Workaround: There is currently no known workaround.
- CSCee36747
Description: If an MWAM is configured to perform IP multicast routing, it will not forward unicast traffic. This only occurs on Processor Complexes (PCs) 3, 5, and 7.
Workaround: Only configure PCs 2, 4, and 6 to forward multicast traffic.
- CSCee87288
Description: Spurious memory accesses during bootup of MWAM processor when Mac authorization feature present.
Workaround: There is currently no known workaround.

- CSCef64412
Description: MWAM processor hangs when a **reload** command is executed from PC while the processor is accessing NVRAM.
Workaround: There is currently no known workaround.
- CSCin80483
Description: Cisco Mobile Wireless application running on a Cisco MWAM on the Catalyst 6500 / Cisco 7600 platform might reload while loading a startup configuration that contains large configurations (for example, IP local pool configuration).
Workaround: Remove the local pool configuration from the startup configuration. This will help prevent the CPUs from reloading. However, with large configurations on MWAM after startup, the CPU can reload later when configured.

Resolved Caveat

The following Cisco MWAM caveats have been resolved with Cisco IOS Release 12.3(8)XU4.

- CSCee45296
Description: When using config on supervisor with the MWAM, the processors are not able to retrieve their configurations from the supervisor. This problem was first seen when using supervisor release 122-18.2.2.SX. This defect would be present in all future supervisor releases when mated with an MWAM IOS image that did not contain this fix.
- CSCef19358
Description: Session to the Cisco MWAM might lockup when a non-default configuration such as “stopbits 1” is used for “line 0” is used.
- CSCef71485
Description: When Cisco Express Forwarding is enabled on a processor image, the Cisco MWAM processor might reload for certain types of traffic, causing IP fragmentation.
- CSCin72286
Description: Multicast packets, fragmented packets and/or tunneled traffic might not be routed and might cause a memory leak. Memory leaks are identified by an error message similar to the following:

```
%SYS-2-MALLOCFAIL: Memory allocation of 1716 bytes failed from 0x2045E1B8, alignment
32
Pool: I/O Free: 1584 Cause: Not enough free memory
Alternate Pool: None Free: 0 Cause: No Alternate pool
```

Related Documentation

Except for feature modules, documentation is available as printed manuals or electronic documents. Feature modules are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 12](#)
- [Platform-Specific Documents, page 12](#)
- [Cisco IOS Software Documentation Set, page 13](#)

Release-Specific Documents

The following documents are specific to Release 12.3 and are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720 and Supervisor Engine 2*
- *Cross-Platform Release Notes for Cisco IOS Release 12.3*

On CCO at:

Technical Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes

- *Caveats for Cisco IOS Release 12.3 T*

See *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.3 and Release 12.3 T.

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Caveats

- Product bulletins, field notices, and other release-specific documents on CCO at:

Technical Documents

Platform-Specific Documents

These documents are available for the Catalyst 6500/Cisco 7600 series platforms on Cisco.com and the Documentation CD-ROM:

- *Cisco Multi-Processor WAN Application Module Installation and Configuration Notes*
- Catalyst 6500 Series Switch Documentation:
 - *Catalyst 6500 Series Switch Module Installation Guide*
 - *Catalyst 6500 Series Switch Installation Guide*
 - *Multi-processor WAN Application Module Installation and Configuration Note*
- Cisco 7600 Series Routers Documentation:
 - *Cisco 7600 Series Internet Router Installation Guide*
 - *Cisco 7600 Series Internet Router Module Installation Guide*
 - *Cisco 7609 Internet Router Installation Guide*

Catalyst 6500 Series Switch Documentation is available at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/index.htm>

Cisco 7600 Series Routers Documentation is available at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guides_books_list.html

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO at:

Technical Documents: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Configuration Guides and Command References

Release 12.3 Documentation Set

You can find the most current Cisco IOS documentation on CCO. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.3



Note

Cisco Management Information Base (MIB) User Quick Reference is no longer published. If you have an account with CCO, you can find the current list of MIBs supported by Cisco. To reach the *Cisco Network Management Toolkit*, go to CCO, press **Login: Technical Support: Software Center: Network Mgmt Software: Cisco Network Management Toolkit: Cisco MIBs**.

Documentation Roadmap for Implementing GGSN Release 5.0 on the Cisco MWAM

The following sections list related documentation (by category and then by task) that will be useful when implementing a Cisco GGSN on the Cisco MWAM platform.

General Overview Documents

Core Cisco 7609 Documents:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_technical_documentation.html

Navigating from Cisco.com: Products & Services / Routers / Cisco 7600 Series Router / Technical Documentation

Cisco 7609 Product Literature (white papers, data sheets, brochures):

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_literature.html

Navigating from Cisco.com: Products & Services / Routers / Cisco 7600 Series Router / Product Literature

Cisco IOS Software Mainline Documentation:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_technical_documentation.html

Navigating from Cisco.com: Products & Services / IOS Software / Cisco IOS Software Releases / Cisco IOS 12.3 Mainline / Technical Documentation

Miscellaneous Cisco IOS Software Documentation:

http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_category_home.html

Documentation List by Task

Getting Started

- *Cisco 7600 Series Internet Router Essentials*
http://www.cisco.com/en/US/products/hw/routers/ps368/products_quick_start09186a0080092248.html
- *Regulatory Compliance and Safety Information for the Cisco 7600 Series Internet Routers*
http://www.cisco.com/en/US/products/hw/routers/ps368/products_regulatory_approvals_and_compliance_list.html

Unpack and install the Cisco 7609 router:

- *Cisco 7609 Internet Router Installation Guide*
http://www.cisco.com/en/US/products/hw/routers/ps368/products_installation_guide_book09186a008007e036.html

Install the Supervisor module and configure the router (basic configuration—VLANs, IP, etc.) using the following documentation:

- *Cisco 7600 Series Internet Router Module Installation Guide*
http://www.cisco.com/en/US/products/hw/routers/ps368/products_module_installation_guide_book09186a008007cd9d.html
- Cisco IOS Software Configuration Guide that applies to the latest release at the time of FCS
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_configuration_guides_list.html

Install and complete the basic Cisco MWAM configuration:

- *Cisco 7600 Series Internet Router Module Installation Guide*
http://www.cisco.com/en/US/products/hw/routers/ps368/products_module_installation_guide_book09186a008007cd9d.html
- *Cisco Multi-processor WAN Application Module Installation and Configuration Note*
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_module_install_config_guide_list.html

Download the Cisco IOS software image containing the GGSN 5.0 feature and configure the GGSNs on the MWAM:

- Cisco GGSN 5.0 Configuration Guide and Command Reference and Associated Release Notes for Cisco IOS Release 12.3(8)XU.
http://www.cisco.com/en/US/products/sw/iosswrel/ps5413/prod_ios_releases_home.html

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/univercd/home/home.htm>

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments 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.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support 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>

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 automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

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

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

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://cisco.com/univercd/cc/td/doc/pcat/>
- *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>
- *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>
- 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.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0411R)

Copyright © 2003-2004, Cisco Systems, Inc.
All rights reserved.