



Release Notes for GGSN 6.0 on the Catalyst 6000 / Cisco 7600 MWAM for Cisco IOS Software Release 12.3(14)YU1

August 30, 2005

Cisco IOS Release 12.3(14)YU1

OL-5266-14

These release notes for the Cisco GGSN Release 6.0 on the Cisco Multi-processor WAN Application Module (MWAM) describe the enhancements provided in Cisco IOS Release 12.3(14)YU1. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.3(14)YU1, see the “[Caveats with Cisco IOS Release 12.3\(14\)YU1](#)” section on page 7 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://www.cisco.com/warp/public/732/docsurvey/rtg/> 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](#)
- [Related Documentation, page 12](#)



Corporate Headquarters:

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

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

- [Limitations, Restrictions, and Important Notes, page 5](#)
- [New and Changed Information, page 7](#)
- [Caveats with Cisco IOS Release 12.3\(14\)YU1, page 7](#)
- [Cisco MWAM Caveats with Cisco IOS Release 12.3\(14\)YU1, page 9](#)
- [Related Documentation, page 12](#)
- [Documentation Roadmap for Implementing GGSN Release 6.0 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 18](#)

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.

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 SGSN communicates between the 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.

Combined 2.5G and 3G packet gateway support and interworking capability on the same node was introduced in Cisco GGSN Release 4.0.

Cisco MWAM Overview

With Cisco IOS Software Release 12.3(2)XB and later, 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(14)YU1 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 5](#)

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.3(14)YU1

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco MWAM on Catalyst 6500 / Cisco 7600	GGSN Standard Feature Set	c6svcmwam-g8is-mz.123-14.YU1.bin	48MB	1 GB	RAM

Hardware and Software Requirements

Proper implementation of the Cisco GGSN features in the Cisco IOS Release 12.3(14)YU1 software requires the following hardware and software:

- Catalyst 6500/Cisco 7600 with a Cisco Supervisor Engine 720 and third-generation policy feature card (PFC3BXL) with integrated Multilayer Switch Feature Card 3 (MSFC3). The MSFC3s must be running the same Cisco IOS software release. The required release is Cisco IOS Release 12.2(18)SXE and later.

For information about Cisco IOS Release 12.2(18)SXE, 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>

- Cisco MWAM, with the 1 GB memory option, in each Cisco 7600 series router. If multiple MWAMs are used, the MWAMs must be running the same Cisco GGSN software release.



Note GGSN Release 5.2, Cisco IOS Release 12.3(14)YQ and later, supports both the standard MWAM 512 MB per processor memory option and the 1 GB per processor memory option.

- IPsec VPN card (if security is a requirement)
- A Cisco Content Services Gateway (CSG) module in each of the Cisco 7600 series routers. The CSGs must be running the same Cisco CSG software release, Release 3.1(3)C6(1) or later.



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(14)YU1, 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(14)YU1, observe the following:

- The number of PDP contexts supported on a GGSN is dependent on the memory and platform in use and the GGSN configuration (for example, whether or not a method of Point to Point Protocol [PPP] has been configured to forward packets beyond the terminal equipment and mobile termination, whether Dynamic Feedback Protocol [DFP] is being used or the memory protection feature is enabled, and what rate of PDP context creation will be supported).



Note

DFP weighs PPP PDPs against IP PDPs with one PPP PDP equal to eight IP PDPs.

For the Cisco 7200 series router, the following list shows the maximum number of PDP contexts supported on the GGSN according to the memory and Cisco 7206 series router in use when no method of PPP has been configured:

- Cisco 7206 VXR NPE-300 with 256 Mb RAM—80,000 IP PDP contexts
- Cisco 7206 VXR NPE-400 router with 512 Mb RAM—135,000 IP PDP contexts

For the Catalyst 6500 series switch/Cisco 7600 series router, the Cisco MWAM can support up to 60,000 IP PDP contexts per GGSN instance, with a maximum of 300,000 IP PDP contexts per MWAM on which five GGSNs are configured.

- Only five instances of the Cisco IOS image 12.3(14)YQ5 image can be loaded onto the MWAM.
- The same image must be loaded onto all processor complexes on the MWAM.
- The session console is provided by a TCP connection from the Supervisor module (no direct console).
- The available memory for bootflash for saving crash information files is 500 KB.
- Only five files can be stored in the bootflash filesystem.
- To avoid issues with high CPU usage, we recommend the following configurations:
 - To reduce the CPU usage during bootup, disable logging to the console terminal by configuring the **no logging console** global configuration command.
 - To ensure that the HRSP interface does not declare itself active until it is ready to process a peer's Hello packets, configure the delay period before the initialization of HSRP groups with the **standby delay minimum 100 reload 100 interface** configuration command under the HRSP interface.
 - To minimize issues with high CPU usage for additional reasons, such as periods of high PPP PDP processing (creating and deleting), disable the notification of interface data link status changes on all virtual template interfaces of the GGSN using the **no logging event link-status interface** configuration command.

```

!
interface Virtual-Template1
description GGSN-VT
ip unnumbered Loopback0
encapsulation gtp
no logging event link-status
gprs access-point-list gprs
end
    
```

For implementation of a service-aware GGSN with Cisco GGSN Release 5.2 and later, the following additional important notes, limitations, and restrictions apply:

- RADIUS accounting is enabled between the CSG and GGSN to populate the Known User Entries Table (KUT) entries with the PDP context user information.
- CSG must be configured with the QS addresses of all the GGSN instances.
- Service IDs on the CSG are configured as numeric strings that match the category IDs on the Diameter Credit Control Application (DCCA) server.
- If RADIUS is not being used, the Cisco CSG is configured as a RADIUS endpoint on the GGSN.
- On the SGSN, the values configured for the number GTP N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, DCCA, and CSG).

Specifically the SGSN $N3 \times T3$ must be greater than:

$2 \times \text{RADIUS timeout} + N \times \text{DCCA timeout} + \text{CSG timeout}$

where:

- 2 is for both authentication and accounting.
- N is for the number of diameter servers configured in the server group.

New and Changed Information

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

- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YU1, page 7](#)
- [New Implementations and Behavior Changes in Cisco IOS Release 12.3\(14\)YU, page 7](#)

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YU1

There are no new implementations or behavior changes in Cisco IOS Release 12.3(14)YU1.

New Implementations and Behavior Changes in Cisco IOS Release 12.3(14)YU

This release of Cisco GGSN Release 6.0 provides support for the following new features:

- Auto-retrieval of charging data records (CDRs) from a Cisco Persistent Storage Device (PSD) (Catalyst 6500/Cisco 7600 platform only)
- High Speed Downlink Data Packet Access (HSDPA) support and associated 3GPP R5 (as required).
- Enhanced Virtual APN (service-aware APN)
- Support for new information elements (IEs) sent from the SGSN (user location, radio access technology (RAT), MS time zone, Customized Application for Mobile Enhanced Logic (CAMEL) charging information, and user location information IEs)
- NPE-G1 support (Cisco GGSN Release 5.0 and later, Cisco 7200 platform)

For information the features in GGSN Release 6.0, see the Cisco IOS Release 12.3(14)YU Cisco GGSN Release 6.0 configuration guide and command reference at:

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

Caveats with Cisco IOS Release 12.3(14)YU1

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(14)YU1.

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(14)YU1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeg03019

Description: When both generic routing encapsulation (GRE) and IP in IP (IPIP) tunnels are configured, and a packet traverses both, Cisco Express Forwarding (CEF) might not work.

Workaround: There is currently no known workaround.
- CSCsa88617

Description: Under some uncharacterized conditions, packets appear on the network that are not normal GTP packets. These packets appear to originate in the PSD and be addressed to the GGSN.

Workaround: There is currently no known workaround.

Resolved Caveats

The following caveats have been resolved in Cisco IOS Release 12.3(14)YU1.

- CSCei33960

Description: After one round of switchover, a newly active Cisco GGSN in a GTP-SR redundant configuration (the previous standby GGSN) might crash during bulk-sync after the new standby GGSN boots up.

The crash might occur after the following sequence of events:

 - a. The GGSN is loaded as standby.
 - b. The standby GGSN recreates PDPs and GTP paths as PDPs are synchronized from the active GGSN.
 - c. The GTP path is deleted on the active GGSN, but the deleted path might fail to synchronize to the standby GGSN.
 - d. While the GTP path is present on the standby GGSN, the same GTP path is created again on the active GGSN because new PDPs are created.
 - e. The new GTP path is synchronized to the standby GGSN.
 - f. After the GTP path is deleted on the standby GGSN, the standby GGSN becomes the new active GGSN after a switchover. If this newly active GGSN performs a bulk synchronization, it crashes.
- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCsb17078

Description: When the **getmany** command is executed on the CISCO-GPRS-ACC-PT-MIB MIB, spurious memory access is seen on the GGSN.

- CSCsb22886

Description: When a charging gateway (CG) sends a redirection message, the GGSN fails to switch the backup CG to the Active CG when the path protocol is TCP.

- CSCsb24007

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCsb39865

Description: With Cisco GGSN Release 5.2 and Release 6.0, the CAUSE IE in the Update PDP Context response from the GGSN is set to 201 (Mandatory IE incorrect) when a Update PDP Context request with a Max Bit Rate (MBR) set to 0 Kbps is received.

Cisco MWAM Caveats with Cisco IOS Release 12.3(14)YU1

This section lists the Cisco MWAM caveats that are open and resolved with Cisco IOS Release 12.3(14)YU1.

Open Caveats

The following Cisco MWAM caveats are open with Cisco IOS Release 12.3(14)YU1.

- CSCee49429

Description: When you reset several MWAM modules, a few of them might go to a PowerDown state with the:

```
%C6KPWR-SP-X-DISABLED: power to module in slot 5 set off (Module Failed SCP dnld)
```

message on the Supervisor console.

Workaround: Power enable the module with the **hw-module module *module-number* reset** command. If it does not enable the card, issue the **power enable module *module-number*** command while in configuration mode.

- CSCeg13327

Description: Forwarding traffic through a GRE tunnel on an MWAM processor causes the output queue interface to be wedged. After starting traffic, the interface gi0/0 output queue reaches max very soon. Thereafter, any attempt to access any device from the MWAM processor (for example, the **ping** command) fails.

This condition occurs when a GRE tunnel is established between two MWAM processors of the same sabyte complex and traffic is passed through. If processors in different complexes are GRE endpoints, the problem does not happen.

Workaround: There is currently no known workaround. The MWAM processor complex has to be reset for accessing to/from this processor. However, it is not a common scenario to establish GRE tunnel between the processors of the same complex.

- CSCeh47418

Description: While remotely executing commands on the MWAM processors from the Supervisor engine module, a debuginfo file might be written to the Supervisor bootflash and the remote console operation might abort. If this condition occurs, memory fragmentation, malloc failure messages, and tracebacks might also be seen.

This condition occurs when the output of the remote command operation is very large.

Workaround: Possible alternatives that can be used include the following:

- Execute the remote command for each processor individually instead of using the **execute-on** command with the **all** keyword option.
- Log onto the MWAM processors individually and execute the **show** commands for which the output is too large for remote execution.
- Direct the output of remote command from the MWAM onto a management VLAN over the switch fabric (Gig0/0 interface) instead of the EOBC interface.

- CSCeh82887

Description: Upon booting an MWAM, Admin Down messages are received for the internal interfaces Gig8/1, Gig8/2, Gig8/3 for the MWAM module on Slot 8. These interfaces are internal interfaces that cannot be configured by the user for disabling traps. Therefore the interfaces should be always shown as Admin Up, and Admin down traps should not be sent.

Additionally, on booting different MWAMs on the chassis, the link status traps conveying Up, Down (and Admin Down which should not be seen) are seen coming in different order for each module.

These traps are seen for the internal interface of each MWAM when the MWAM is reset.

Workaround: There is currently no known workaround.
- CSCin85669 (duplicate of CSCeg04173)

Description: When an MWAM module is shut down, error bits do not get set for the variable module TestResult.

Workaround: There is currently no known workaround.
- CSCsa50215

Description: Unable to access MWAM processor via session or telnet command for 10 minutes after the processor has been reloaded.

Workaround: Configure the **ip rcmd rcp-enabled** command on the supervisor module.

Resolved Caveats

The following Cisco MWAM caveats have been resolved with Cisco IOS Release 12.3(14)YU1.

- CSCin89403

Description: An MWAM processor does not see the other MWAM processors of a different complex as CDP neighbors. This condition occurs in the Sup22. Each MWAM processor sees just the Supervisor and the MWAM processor of the same complex as CDP neighbors.
- CSCsa48606

Description: The **execute-on slot-num** command does not retrieve complete output for the show tech-support on processor 1.

Unreproducible Caveat

The Cisco MWAM caveat listed in this section has not been reproduced during testing with Cisco GGSN Release 6.0, Cisco IOS Release 12.3(14)YU1. In the unlikely event you experience the problem described in this section, please contact Cisco customer service.

- CSCeh58857

Description: The **execute-on** command locks up the direct Telnet connection to the MWAM processors. When this condition occurs, the direct Telnet access to the MWAM processors will fail with a series of %Bad Password Entered messages, even though none were entered.

This condition occurs after entering the Supervisor console command **execute-on** to the MWAMs. It also happens when access-lists are used on VTY lines to limit Telnet access to only trusted-source IP addresses.

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 13](#)
- [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 Documents: 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

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Caveats



Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco Bug Toolkit: Cisco Bugtool Navigator II**, or at <http://www.cisco.com/support/bugtools>.

- 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 and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

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 and the Documentation CD-ROM. 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 6.0 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 feature set and configure the GGSNs on the MWAM:

- Cisco GGSN 6.0 Configuration Guide and Command Reference and Associated Release Notes for Cisco IOS Release 12.3(14)YU1.
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/moblwrls/ggsn/index.htm>

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, CCVP, 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, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0502R)

Copyright © 2003-2005, Cisco Systems, Inc.
All rights reserved.