



Release Notes for Cisco 7000 Family for Cisco IOS Release 12.3 XU

January 26, 2005

Cisco IOS Release 12.3(8)XU4

OL-6595-03

These release notes for the Cisco 7000 family 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 for Cisco IOS Release 12.3 XU” section on page 8](#) and *Caveats for Cisco IOS Release 12.3*. 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.

Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 6](#)
- [MIBs, page 7](#)
- [Caveats for Cisco IOS Release 12.3 XU, page 8](#)
- [Related Documentation, page 24](#)
- [Obtaining Documentation, page 30](#)
- [Obtaining Technical Assistance, page 31](#)



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

Copyright © 2004-2005. Cisco Systems, Inc. All rights reserved.

System Requirements

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

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Support, page 4](#)

Memory Recommendations

Table 1 Memory Recommendations for the Cisco IOS Release 12.3(8)XU4

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	GGSN Standard Feature Set	c7200-g8is-mz	48 MB	512 MB	RAM
		c7200-g8ik8s-mz	48 MB	512 MB	RAM
		c7200-g8ik9s-mz	48 MB	512 MB	RAM

Table 2 Memory Recommendations for the Cisco IOS Release 12.3(8)XU3

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	GGSN Standard Feature Set	c7200-g8is-mz	48 MB	512 MB	RAM
		c7200-g8ik8s-mz	48 MB	512 MB	RAM
		c7200-g8ik9s-mz	48 MB	512 MB	RAM

Table 3 Memory Recommendations for the Cisco IOS Release 12.3(8)XU2

Platforms	Feature Sets	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	GGSN Standard Feature Set	c7200-g8is-mz	48 MB	512 MB	RAM
		c7200-g8ik8s-mz	48 MB	512 MB	RAM
		c7200-g8ik9s-mz	48 MB	512 MB	RAM

Supported Hardware

Cisco IOS Release 12.3(8)XU4 supports the following Cisco 7000 platforms:

- Cisco 7200 series routers

For detailed descriptions of the new hardware features, see the “[New and Changed Information](#)” section on page 6.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7200 series software image with Cisco IOS Release 12.3(8)XU4:

```
Router> show version
Cisco IOS Software, 7301 Software (c7200-g8is-mz), Version 12.3(8)XU4, RELEASE
SOFTWARE (fc1)
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, please refer to *How to Choose a Cisco IOS Software Release* at:

http://www.cisco.com/warp/public/130/choosing_ios.shtml

For information about upgrading to a new software release, refer to the appropriate platform-specific document:

Cisco 7200 Series, 7300 Series, 7400 Series, and 7500 Series Routers

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094c07.shtml

For *Cisco IOS Upgrade Ordering Instructions*, refer to the document at the following location:

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

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.



Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

The feature set tables have been removed from the Cisco IOS Release 12.3 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

<http://www.cisco.com/support/FeatureNav/FNFAQ.html>

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.3 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Feature**.
 - Step 2** To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.
 - Step 3** Select a feature from the left text box, and click the **Add** button to add a feature to the Selected Features text box on the right side of the web page.



Note To learn more about a feature in the list, click the **Description** button below the left box.

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

- Step 4** Click **Continue** when you are finished selecting features.
 - Step 5** From the Major Release drop-down menu, choose **12.3**.
 - Step 6** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 7** From the Platform Family drop-down menu, select the appropriate hardware platform. The “Your selections are supported by the following:” table will list all the software images (feature sets) that support the feature(s) that you selected.
-

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.3, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Compare/Release**.
 - Step 2** In the “Find the features in a specific Cisco IOS release, using one of the following methods:” box, choose **12.3** from the Cisco IOS Major Release drop-down menu.
 - Step 3** Click **Continue**.
 - Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 5** From the Platform Family drop-down menu, choose the appropriate hardware platform.
 - Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. The “Your selections are supported by the following:” table will list all the features that are supported by the feature set (software image) that you selected.
-

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family of routers for Cisco IOS Release 12.3 XU:

New Hardware Features in Cisco IOS Release 12.3(8)XU4

There are no new hardware features supported in Cisco IOS Release 12.3(8)XU4.

New Software Features in Cisco IOS Release 12.3(8)XU4

There are no new software features supported in Cisco IOS Release 12.3(8)XU4.

New Hardware Features in Cisco IOS Release 12.3(8)XU3

There are no new hardware features supported in Cisco IOS Release 12.3(8)XU3.

New Software Features in Cisco IOS Release 12.3(8)XU3

There are no new software features supported in Cisco IOS Release 12.3(8)XU3.

New Hardware Features in Cisco IOS Release 12.3(8)XU2

The following new hardware feature is supported in Cisco IOS Release 12.3(8)XU2:

Cisco 7200 Series Routers

The Cisco 7200 Series Routers deliver exceptional performance/price, modularity, and scalability in a compact form factor with a wide range of deployment options. With processing speeds up to 1 million packets per second, port adapters ranging from NxDS0 to OC-12, and an unparalleled number of high-touch IP services, the Cisco 7200 is the ideal WAN edge device for enterprises and service providers deploying any of the following solutions:

- WAN Edge—Award-winning quality-of-service (QoS) feature performance
- Broadband Aggregation—Up to 16,000 Point-to-Point Protocol (PPP) sessions per chassis
- Multiprotocol Label Switching provider edge (MPLS PE)—Solutions for provider edge deployment
- Voice/Video/Data integration—Time-division multiplexer (TDM)-enabled VXR chassis and voice port adapters
- IP Security virtual private networking (IPSec VPN)—Scalable to 5,000 tunnels per chassis
- High-end Customer Premise Equipment (CPE)

The Cisco 7200 addresses these solution requirements by integrating functions previously performed by separate devices into a single platform. Through this integration, the Cisco 7200 provides a single, cost-effective platform that supports:

- High-density LAN and WAN interfaces
- Broadband Subscriber services aggregation—including PPP, RFC1483 termination and Layer 2 Tunneling Protocol (L2TP) tunneling
- Digital T1/E1 TDM trunk termination for voice, video and data.
- High-density multichannel T3/E3 and T1/E1 with integrated channel service unit/data service unit (CSU/DSU)
- ATM, Packet over SONET (POS) and Dynamic Packet Transport (DPT) connectivity
- Direct ATM Circuit Emulation Standard (CES) connectivity for voice, video, and data
- Direct IBM mainframe channel connectivity
- Light-density Layer 2 Ethernet switching

New Software Features in Cisco IOS Release 12.3(8)XU2

There are no new software features supported in Cisco IOS Release 12.3(8)XU2.

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>.

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 4](#).

Table 4 *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB

Table 4 *Deprecated and Replacement MIBs (continued)*

Deprecated MIB	Replacement
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Caveats for Cisco IOS Release 12.3 XU

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 12.3 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.



Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, **log in** to Cisco.com and click **Service and Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

Because Cisco IOS Release 12.3(2)XB is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

Table 5 Caveats Reference for Cisco IOS Release 12.3 XU

DDTS Number	Open in Release	Resolved in Release
CSCdw08251		12.3(8)XU4
CSCeb40999	12.3(8)XU2, 12.3(8)XU3	
CSCed78149		12.3(8)XU2
CSCee22639		12.3(8)XU4
CSCee48984		12.3(8)XU2
CSCee66737		12.3(8)XU2
CSCee67450		12.3(8)XU4
CSCee70524		12.3(8)XU2
CSCee87603	12.3(8)XU2, 12.3(8)XU3	
CSCee88746	12.3(8)XU2, 12.3(8)XU3	
CSCee93335	12.3(8)XU2, 12.3(8)XU3	
CSCee94797	12.3(8)XU2, 12.3(8)XU3	
CSCef05237		12.3(8)XU2
CSCef09121		12.3(8)XU2
CSCef09421	12.3(8)XU2, 12.3(8)XU3	
CSCef12356		12.3(8)XU2
CSCef19117		12.3(8)XU4
CSCef21387		12.3(8)XU2
CSCef26071		12.3(8)XU2
CSCef29307	12.3(8)XU2, 12.3(8)XU3	
CSCef30823	12.3(8)XU2, 12.3(8)XU3	
CSCef31241	12.3(8)XU2, 12.3(8)XU3	
CSCef32820	12.3(8)XU2, 12.3(8)XU3	
CSCef32893	12.3(8)XU2, 12.3(8)XU3	
CSCef37928		12.3(8)XU2
CSCef38295		12.3(8)XU2
CSCef44957	12.3(8)XU2, 12.3(8)XU3	

Table 5 Caveats Reference for Cisco IOS Release 12.3 XU (continued)

CSCef45905		12.3(8)XU2
CSCef48312		12.3(8)XU2
CSCef58110		12.3(8)XU2
CSCef62287		12.3(8)XU2
CSCef64140		12.3(8)XU2
CSCef69920		12.3(8)XU2
CSCef77001		12.3(8)XU3
CSCef85677		12.3(8)XU3
CSCeg01375	12.3(8)XU3	
CSCeg08927		12.3(8)XU4
CSCeg11985		12.3(8)XU3
CSCeg18250		12.3(8)XU4
CSCeg41118		12.3(8)XU4
CSCin74608	12.3(8)XU2, 12.3(8)XU3	
CSCin74810		12.3(8)XU3
CSCin76672	12.3(8)XU2, 12.3(8)XU3	
CSCin77875	12.3(8)XU2	
CSCin78024		12.3(8)XU2
CSCin78980		12.3(8)XU2
CSCin82407		12.3(8)XU3

Open Caveats—Cisco IOS Release 12.3(8)XU4

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.

There are no known open caveats for Cisco IOS Release 12.3(8)XU4.

Resolved Caveats—Cisco IOS Release 12.3(8)XU4

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

- CSCdw08251

The cause value in CREATE PDP RESPONSE failure case is incorrect.

This issue occurs when radius servers are down and the APN requested by the user is in non-transparent mode.

There are no known workarounds.

- CSCee22639

When the **ip tcp adjust-mss** option is used on a Cisco IOS router, and there is IP fragmentation, data corruption may occur on some IP fragments. The corruption happens in such a way that it is not detected by the TCP checksum.

This issue only occurs if the **ip tcp adjust-mss** option is used, and if there is fragmentation, and with certain payload data.

Workaround: Avoid IP fragmentation, or disable the **ip tcp adjust-mss**.



Note Having fragmentation in case TCP MSS is specifically adjusted to avoid it is an anomaly situation which should be investigated in the network separately.

- 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

A Cisco router configured with the **ip tcp adjust-mss** command may fail to set the value for outbound packets. The command works on 12.3(7)T2 code, but fails on for the 12.3(8)T code.

This issue is observed on a Cisco 3700 router.

Workaround: Disable cef. However, this can affect performance on the router.

- CSCeg08927

A Cisco GGSN running 12.3(8)T3 GPRS software unexpectedly reloads in some cases involving repetitive create PDP context requests on an existing PDP in GGSN.

This issue is observed when the following sequence occurs.

1. A successful create PDP request and PDP is created.
2. A second create PDP request on the same PDP requesting DNS Address but some error in PCO, as a result this create request is rejected.
3. A third create PDP request without PCO

There are no known workarounds.

- CSCeg18250

GGSN reloads when the peer sends data into the control path.

This issue is observed on a Cisco router configured for General Packet Radio Service (GPRS) and runs GGSN Release 4.0 when the following conditions occur:

- The peer (SGSN or GTP-relay box) send data packet into control path
- A GTP relay device is placed in between the GGSN and the SGSNs

There are no known workarounds.

- CSCeg41118

A Cisco router running Cisco gateway GPRS support node software (GGSN) may unexpectedly reload if an incorrect GPRS tunneling protocol version 1 (GTPv1) PDP context delete request is received with Tunnel End-point identifier (TEID) set to data-teid that has been assigned by GGSN instead of Control TEID.

This issue only occurs if some data has passed through the PDP in downlink direction.

Workaround: Correct the SGSN to send the correct TEIDc instead of TEIDd.

Open Caveats—Cisco IOS Release 12.3(8)XU3

This section documents possible unexpected behavior by Cisco IOS Release 12.3(8)XU3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb40999

If DHCP server fails to respond to a DHCP request, and “peer default ip address dhcp” is configured on the virtual-template, then the lease server address will be printed as 0.0.0.0 in the output of “debug dhcp detail”. This does not mean that the request was not sent to the server.

There are no known workarounds.

- CSCee87603

Memory allocation fails with Trace back when GGSN tries to deletes pdp.

This issue only occurs when DHCP server not able to renew all request from GGSN.

There are no known workarounds.

- CSCee88746

GGSN is displaying “gprs charging cdr-option sgsn-plmn” configuration in show run with out configuring it.

This is occurs in the following sequence:

1. Configure “gprs charging cdr-option sgsn-plmn”
2. Disable “service gprs ggsn” without unconfiguring configuration 1
3. Enable “service gprs ggsn”

Workaround: Disable “gprs charging cdr-option sgsn-plmn” before disabling GGSN service.

- CSCee93335

When a Cisco router is running GGSN software with PDP PPP/L2TP, the DSCP on outer IP header may not be marked correctly in downlink direction.

There are no known workarounds.

- CSCee94797

A Cisco router running GGSN R5.0 software increments both Optional IE Invalid and Optional IE Incorrect counter.

This issue occurs when the PCO in the create PDP request contains two CHAP messages both having a code of “Response” and the username in both the messages are different. This is a very unusual scenario to occur.

There are no known workarounds.

- CSCef09421

There are two issues with trashing the CDRs and gprs maintenance mode:

1). When only gprs (Box level) maintenance mode is configured and charging service mode is still operational, the command to trash all the CDRs, i.e. “gprs charging cdr all no-transfer” succeeds and CDRs get cleared.

2). If there is a CDR in the pending queue, then trying to trash the CDR only in the gprs service mode (while charging mode is operational) gives an error message that there are no CDRs even though the CDR is still there.

These issues occur when only gprs service mode is maintenance and the charging service mode is operational.

Workaround: Configure both gprs charging service mode and gprs service mode for maintenance and then trash the CDRs.

- CSCef29307

Cisco GGSN does not clear the TCP socket from the GGSN to the Charging Gateway and, hence, does not respond to the Nodealive requests from the Charging gateway; under the condition that the Charging Functionality is under a lot stress and the charging Gateway is going up and down frequently, resulting in a lot of charging data records being queued.

Workaround: Execute the **show tcp brief** command. Then clear the tcb using the command **clear tcp tcb <tcb value from the show tcp brief command>** command. Now send Nodealive from the Charging Gateway.

- CSCef30823

A Cisco router running R5.0 GGSN software reject the duplicate gtpv1 primary pdp context with TFT information when the “gprs gtp create-request v1 update-existing-pdp cli” is enabled.

This issue only occurs when the primary pdp context comes with TFT information and when the “gprs gtp create-request v1 update-existing-pdp” cli enabled.

There are no known workarounds.

- CSCef31241

GGSN adds extra byte(00) before LRSN value.

GGSN is adding one extra byte before LRSN value and converting LRSN into 5 byte value. According to spec(32.215 page 37), LRSN number should be unsigned integer of four octets.

There are no known workarounds.

- CSCef32820

Cisco GGSN Deletes and create the PDP context again under the condition that the new create request for an already existing context is coming for GTPv0, and that it is coming from a different SGSN than the earlier one and that this new SGSN already is having a few active contexts with the same GGSN and the Restart count value in this new create request is different.

There are no known workarounds.

- CSCef32893

The GGSN IMS related process holds memory even after no service gprs ggsn and holds memory even after unconfiguring service gprs ggsn.

There are no known workarounds.

- CSCef44957
data_msg_dropped counter is not incremented on receiving invalid ip packet.
This issue occurs when data_msg_dropped counter is not incremented in “sh gprs gtp stat” output on receiving invalid ip packet.
There are no known workarounds.
- CSCeg01375
Cisco GGSN shows variation in the value of PDP creation time in the output of **show gprs gtp pdp tid <id>** CLI.
This occurs when the above mentioned CLI is executed multiple times randomly. This fluctuation does not impact charging aspects for the PDP context.
There are no known workarounds.
- CSCin74608
GGSN may reload due to memory corruption.
This issue is only seen when the test is ran on one particular MWAM card, It can not be reproduce in other MWAM or c7200 routers.
There are no known workarounds.
- CSCin76672
On a Cisco Gateway GPRS Support Node (GGSN), for a PPP (Point-to-Point Protocol) type PDP (Packet Data Protocol) context where the PPP session endpoint is on GGSN, if the MS (Mobile Station) deletes the PPP session by sending LCP TERMREQ, the “cause for record closing” used by GGSN in the associated CDR (Charging Data Record) is “abnormalRelease”.
This happens for PPP type PDP context where MS initiates session deletion by sending PPP LCP TERMREQ. If instead the MS initiates closing by sending GTP PDP delete request message to GGSN, the problem is not seen, i.e. the cause code used in CDR is normal Release.
There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.3(8)XU3

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(8)XU3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCef77001

G-CDR duration time can have an inaccuracy of +/- 1sec from the difference between CDR opening and closure times present in CDR.

This occurs randomly with most of the CDRs having correct duration time and some CDRs having inaccurate time.

There are no known workarounds.

- CSCef85677

When encountering a large number of volume thresholds, the number of events that were generated were also high; causing chunk malloc to allocate some memory to process the event. Under high volume of events, the whole defined chunk would get used and subsequent events will not be honored and trace backs were seen.

Workaround: Rather than using chunk malloc, use managed chunk malloc. This will allow the defined chunk to increase dynamically when usage of chunk memory goes beyond a defined threshold. Subsequent to making changes, no traces were observed.

- CSCeg11985

The following config in charging profile does not show up in the running config and will be lost after reload:

```
limit volume 1048576 reset
```

This issue only occurs when the value of 1048576 is configured, which is the default volume trigger.

Workaround: Use 1000000 or something other than 1048576. If 1048576 must be used with the reset option, then enter it after each reload.

- CSCin74810

This issue occurs on a GGSN Release R5.0 with the use of framed protocol GPRS_PDP_CONTEXT in a user profile on RADIUS.

While a PPP PDP context for this profile is created and authenticated on the GGSN, authentication fails with an error message stating that this framed protocol is not allowed.

Workaround: Use framed protocol PPP in the user profile.

- CSCin82407

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

Open Caveats—Cisco IOS Release 12.3(8)XU2

This section documents possible unexpected behavior by Cisco IOS Release 12.3(8)XU2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb40999

If DHCP server fails to respond to a DHCP request, and “peer default ip address dhcp” is configured on the virtual-template, then the lease server address will be printed as 0.0.0.0 in the output of “debug dhcp detail”. This does not mean that the request was not sent to the server.

There are no known workarounds.

- CSCee87603

Memory allocation fails with Trace back when GGSN tries to deletes pdp.

This issue only occurs when DHCP server not able to renew all request from GGSN.

There are no known workarounds.

- CSCee88746

GGSN is displaying “gprs charging cdr-option sgsn-plmn” configuration in show run with out configuring it.

This is occurs in the following sequence:

1. Configure “gprs charging cdr-option sgsn-plmn”
2. Disable “service gprs ggsn” without unconfiguring configuration 1
3. Enable “service gprs ggsn”

Workaround: Disable “gprs charging cdr-option sgsn-plmn” before disabling GGSN service.

- CSCee93335

When a Cisco router is running GGSN software with PDP PPP/L2TP, the DSCP on outer IP header may not be marked correctly in downlink direction.

There are no known workarounds.

- CSCee94797

A Cisco router running GGSN R5.0 software increments both Optional IE Invalid and Optional IE Incorrect counter.

This issue occurs when the PCO in the create PDP request contains two CHAP messages both having a code of “Response” and the username in both the messages are different. This is a very unusual scenario to occur.

There are no known workarounds.

- CSCef09421

There are two issues with trashing the CDRs and gprs maintenance mode:

1). When only gprs (Box level) maintenance mode is configured and charging service mode is still operational, the command to trash all the CDRs, i.e. “gprs charging cdr all no-transfer” succeeds and CDRs get cleared.

2). If there is a CDR in the pending queue, then trying to trash the CDR only in the gprs service mode (while charging mode is operational) gives an error message that there are no CDRs even though the CDR is still there.

These issues occur when only gprs service mode is maintenance and the charging service mode is operational.

Workaround: Configure both gprs charging service mode and gprs service mode for maintenance and then trash the CDRs.

- CSCef29307

Cisco GGSN does not clear the TCP socket from the GGSN to the Charging Gateway and, hence, does not respond to the Nodealive requests from the Charging gateway; under the condition that the Charging Functionality is under a lot stress and the charging Gateway is going up and down frequently, resulting in a lot of charging data records being queued.

Workaround: Execute the **show tcp brief** command. Then clear the tcb using the command **clear tcp tcb <tcb value from the show tcp brief command>** command. Now send Nodealive from the Charging Gateway.

- CSCef30823

A Cisco router running R5.0 GGSN software reject the duplicate gtpv1 primary pdp context with TFT information when the “gprs gtp create-request v1 update-existing-pdp cli” is enabled.

This issue only occurs when the primary pdp context comes with TFT information and when the “gprs gtp create-request v1 update-existing-pdp” cli enabled.

There are no known workarounds.

- CSCef31241

GGSN adds extra byte(00) before LRSN value.

GGSN is adding one extra byte before LRSN value and converting LRSN into 5 byte value. According to spec(32.215 page 37), LRSN number should be unsigned integer of four octets.

There are no known workarounds.

- CSCef32820

Cisco GGSN Deletes and create the PDP context again under the condition that the new create request for an already existing context is coming for GTPv0, and that it is coming from a different SGSN than the earlier one and that this new SGSN already is having a few active contexts with the same GGSN and the Restart count value in this new create request is different.

There are no known workarounds.

- CSCef32893

The GGSN IMS related process holds memory even after no service gprs ggsn and holds memory even after unconfiguring service gprs ggsn.

There are no known workarounds.

- CSCef44957
data_msg_dropped counter is not incremented on receiving invalid ip packet.
This issue occurs when data_msg_dropped counter is not incremented in “sh gprs gtp stat” output on receiving invalid ip packet.
There are no known workarounds.
- CSCin74608
GGSN may reload due to memory corruption.
This issue is only seen when the test is ran on one particular MWAM card, It can not be reproduce in other MWAM or c7200 routers.
There are no known workarounds.
- CSCin76672
On a Cisco Gateway GPRS Support Node (GGSN), for a PPP (Point-to-Point Protocol) type PDP (Packet Data Protocol) context where the PPP session endpoint is on GGSN, if the MS (Mobile Station) deletes the PPP session by sending LCP TERMREQ, the “cause for record closing” used by GGSN in the associated CDR (Charging Data Record) is “abnormalRelease”.
This happens for PPP type PDP context where MS initiates session deletion by sending PPP LCP TERMREQ. If instead the MS initiates closing by sending GTP PDP delete request message to GGSN, the problem is not seen, i.e. the cause code used in CDR is normalRelease.
There are no known workarounds.
- CSCin77875
When a PPP over GTP session terminates on a virtual-access interface on the GGSN and idle timer is configured to run on it, some uplink traffic going through GTP reaching this virtual-access interface does not reset its PPP idle timer, causing idle expiration even in the presence of traffic. Then this active PPP PDP got deleted.
This problem exists in Release 5.0 of Cisco GGSN.
This issue may occur occasionally. There are no know workarounds as long as the PPP idle timer is used.

Resolved Caveats—Cisco IOS Release 12.3(8)XU2

All the caveats listed in this section are resolved in Cisco IOS Release 12.3(8)XU2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCed78149

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCee48984

Because of the new supported change request 311 of standard (in GGSN R4.0 for gtpv1), if a new request is create on an existing PDP, the exiting PDP will be deleted and a new PDP will be created according to the new create request.

However, if the request is retransmitting (maybe the create response and the retry create crosses the wire), then it is not recommend that the PDP be deleted and recreated.

There are no known workarounds.

- CSCee66737

Bad packet dump occurs when debug gprs charging packet is enabled.

This issue occurs when TCP is used for charging protocol. On the simulator, the protocol was UDP. Some pending CDRs were generated by sending node-alive from the CG, causing the pending CDRs to accumulate.

Workaround: Do not enabled debug gprs charging packet.

- CSCee70524

In GGSN software, if the “aggregate route” feature is configured on an APN and there are some PDP using that aggregate route, sending down stream traffic to a non-exit PDP address that matches the aggregate route will cause performance degradation.

Workaround: Do not configure the “aggregate route” feature. However, this will affect the activation rate.

- CSCef05237

GGSN will not accept the charging characteristics value sent in create request and will create PDP context with GGSN default values.

This issue may occur when any of the first 4 bits of the charging characteristics sent in create request is set.

Workaround: Always keep the first 4 bits of charging characteristics at “0”.

- CSCef09121

Cisco GGSN unexpectedly reloads when GTPv1 primary pdp context is deleted before the very next lease renewal.

This issue occurs under the following condition:

- 1) Create a v1 PDP using DHCP.
- 2) delete the above PDP. This will trigger DHCP to put the address lease in “holddown” state for 5 seconds.
- 3) Immediately create a new V1 PDP by repeating the call of step#1 (same msisdn, apn, nsapi, etc.). This must be done within 5 second of step #2.
- 4) Create a secondary PDP tied to the primary PDP created in step #3.
- 5) Delete the primary PDP created in step #3.

Steps 4 and 5 must be perform before the very next lease renewal after Step 2.

There are no known workarounds.

- CSCef12356

On Cisco router running Gateway GPRS Support Node (GGSN) R5.0 image, with Hanging PDP feature enabled, it is observed that Accounting Stop record is sent out when hanging PDP context is deleted.

There are no known workarounds.

- CSCef21387

Under rare condition, when the Cisco router is running GGSN R5.0, there might be some PDP contexts that can not be deleted.

This issue occurs when Open/Close PDP contexts are in a high rate while sending high rate traffic to active PDP contexts in both directions.

There are no known workarounds.

- CSCef26071
A Cisco router running Gateway general packet radio service (GPRS) Support Node (GGSN) may return the wrong error type when trying to create more than one home PLMN entry using snmp set. This issue occurs when a Cisco router running Gateway general packet radio service (GPRS) Support Node (GGSN) return commitFailed instead of inconsistent Value error when trying to create more than one home PLMN entry in cGgsnPlmnTable.
There are no known workarounds.
- CSCef37928
GGSN reloads while creating multiple pdp.
This issue occurs when dhcp local pool is configured for ip address allocation and loopback interface sends multiple create request.
When this happens, GGSN reloads with traceback.
There are no known workarounds.
- CSCef38295
This problem is not a defect, but an inconsistency in the formats of the CLI and Vendor Specific Attribute used for the hanging PDP feature of Cisco's GGSN. This feature has been added via Release 5.0.
These changes are actually external interface improvements and have no workaround.
- CSCef45905
GGSN will allow PDP contexts to open without CDR, even though the charging functionality of GGSN is used.
This issue occurs when we remove the CG configuration of active GGSN in charging maintenance mode and pdp create request comes before configuring a new CG.
There are no known workarounds.
- CSCef48312
When no-partial-cdr-generation and sgsn-change-limit are configured, if the CDR is closed by a non-sgsn-change trigger, the current SGSN is missing in the new CDR even though this SGSN has been used during this CDR period. Since SGSN address is mandatory in R4, it should not be omitted even though it has not changed. The SGSN list may also be missing if there is no new SGSN in this CDR and it is closed by another non-sgsn-change trigger.



Note This is a documented behavior, but since in R4 (the parameter has changed to mandatory) it should be changed to ensure that if an SGSN is used by this CDR, it should appear in the list even though it has not changed.

- CSCef58110
The problem of this defect is that when a GTPv1 Create Request comes to a Cisco GGSN, which is either entirely in maintenance mode or has the corresponding APN for this Request in maintenance mode, the GGSN returns a negative Create Response with a cause code already obsolete in the UMTS standard. This obsolete cause is “service not available”, which should be “resource not available” according to the standard.
This problem impacts Cisco GGSN Release 4.0.
There are no known workarounds.

- CSCef62287

When the **gprs charging cdr-option no-partial-cdr-generation** command is configured after open or closed CDRs already exists, the CDRs may have some incorrect fields with zero length and no value.

This issue is observed on a Cisco platform that functions as a GGSN.

Workaround: Do not change the CDR configuration when CDRs already exist in the memory. If you must change the CDR configuration, first clear all PDPs and CDRs.

- CSCef64140

This problem is about Cisco GGSN's disabling of the GTP idle timer for all PPP-Regenerated PDP contexts so that the GGSN does not have a means to idle timeout such contexts. The resolution for this problem is to enable this timer for such contexts whenever the idle timing functionality is configured at the APN or/and the global levels. If both levels have it configured, the value and direction configured at the APN level take precedence.

This problem impacts Cisco GGSN's Release 5.0. Before this resolution is implemented, the only place to time a PPP-Regenerated context's idleness is on the LNS/PDN.

There are no known workarounds.

- CSCef69920

If the "gprs charging cdr-option no-partial-cdr-generation" is configured, and there is a SGSN change limit trigger configured; either using the global "gprs charging container sgsn-change-limit <n>" or under the charging profile "limit sgsn-change, the CDR will not have any SGSN address in the CDR if the CDR is closed due to a non-sgsn-change trigger and there is no SGSN change in this CDR.

In r99, not all the mandatory fields are required to be present. The original intention was to avoid having repeated SGSN addressed in combined list of SGSN address from all the partial CDRs, when the SGSN change limit is configured. However, that leaves some CDRs (as in the case described above) without SGSN address. Even the SGSN address used by this CDR.

In r4 the Spec this is a mandatory field and that has been implemented.

This DDTs gives that behavior even for pre r4 cases, by introducing the following CLI:

```
gprs charging cdr-option no-partial-cdr-generation all
```

When the new keyword "all" is specified, the SGSN address will be filled in the CDR, even if it has not changed, regardless of the charging release.

There are no known workarounds.

- CSCin78024

A Cisco Router running R5.0 software may fail to send the current active CG address in the Accounting Stop Record.

This issue occurs after sending a Redirection Request with a different CG as the recommended node after creating a context.

There are no known workarounds.

- CSCin78980

A Cisco router running R5.0 GGSN software may fail to send the current QoS and SGSN address after a handoff in the Accounting Stop Record.

This issue occurs only after a handoff from GTPv0 to GTPv1 or from GTPv1 to GTPv0.

Workaround: When "aaa-accounting interim update" is configured, this issue is not seen.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family of routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 24](#)
- [Platform-Specific Documents, page 25](#)
- [Feature Modules, page 25](#)
- [Cisco IOS Software Documentation Set, page 26](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.3*

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes

On the Documentation CD-ROM at:

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

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

Technical Documents

- *Caveats for Cisco IOS Release 12.3(8)XU4*

As a supplement to the caveats listed in “[Caveats for Cisco IOS Release 12.3 XU](#)” in these release notes, see *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: 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 Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Select & Download Software: Jump to a software resource: Software Bug Toolkit/Bug Watcher**. Another option is to go to <http://www.cisco.com/support/bugtools/bugtool.shtml>.

Platform-Specific Documents

These documents are available for the Cisco 7000 family of routers on Cisco.com and the Documentation CD-ROM:

- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7200 Routers Quick Start Guide*

On Cisco.com at:

Technical Documents: All Product Documentation: Core/High-End Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: All Product Documentation: Core/High-End Routers

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.3(8)XU4 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: New Feature Documentation

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

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. The Cisco IOS software documentation set is 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 one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and 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 Cisco.com at:

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

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.3: Configuration Guides and Command References

Cisco IOS Release 12.3 Documentation Set Contents

[Table 6](#) lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.



Note

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

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.3

On the Documentation CD-ROM at:

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

Table 6 Cisco IOS Release 12.3 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • Cisco IOS Configuration Fundamentals Configuration Guide • Cisco IOS Configuration Fundamentals Command Reference 	Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • Cisco IOS Bridging and IBM Networking Configuration Guide • Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2 • Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2 	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
<ul style="list-style-type: none"> • Cisco IOS Dial Technologies Configuration Guide: Dial Access • Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications • Cisco IOS Dial Technologies Command Reference, Volume 1 of 2 • Cisco IOS Dial Technologies Command Reference, Volume 2 of 2 	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • Cisco IOS IP Configuration Guide • Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services • Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols • Cisco IOS IP Command Reference, Volume 3 of 3: Multicast 	IP Addressing IP Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • Cisco IOS AppleTalk and Novell IPX Configuration Guide • Cisco IOS AppleTalk and Novell IPX Command Reference 	AppleTalk Novell IPX

Table 6 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide • Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference 	<p>Apollo Domain Banyan VINES DECnet ISO CLNS XNS</p>
<ul style="list-style-type: none"> • Cisco IOS Voice, Video, and Fax Configuration Guide • <i>Cisco IOS Voice, Video, and Fax Command Reference</i> 	<p>Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support</p>
<ul style="list-style-type: none"> • Cisco IOS Quality of Service Solutions Configuration Guide • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	<p>Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms</p>
<ul style="list-style-type: none"> • Cisco IOS Security Configuration Guide • <i>Cisco IOS Security Command Reference</i> 	<p>AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs</p>
<ul style="list-style-type: none"> • Cisco IOS Switching Services Configuration Guide • Cisco IOS Switching Services Command Reference 	<p>Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation</p>
<ul style="list-style-type: none"> • Cisco IOS Wide-Area Networking Configuration Guide • Cisco IOS Wide-Area Networking Command Reference 	<p>ATM Frame Relay SMDS X.25 and LAPB</p>
<ul style="list-style-type: none"> • Cisco IOS Mobile Wireless Configuration Guide • Cisco IOS Mobile Wireless Command Reference 	<p>General Packet Radio Service</p>

Table 6 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • Cisco IOS Terminal Services Configuration Guide • Cisco IOS Terminal Services Command Reference 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • Cisco IOS Debug Command Reference • Cisco IOS Software System Error Messages • <i>New Features in 12.3-Based Limited Lifetime Releases</i> • New Features in Release 12.3 T • Release Notes (Release note and caveat documentation for 12.3-based releases and various platforms) 	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco products documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 24.

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

All other trademarks mentioned in this document or Web site 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. (0301R)

Copyright © 2004-2005
 Cisco Systems, Inc.
 All rights reserved.