Release Notes for Cisco 7000 Series Routers for Cisco IOS Release 12.2 YW

January 13, 2004

Cisco IOS Release 12.2(8)YW3

OL-1620-04

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(8)YW3. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(8)YW3, see the "Caveats for Cisco IOS Release 12.2 YW" section on page 12 and *Caveats for Cisco IOS Release 12.2 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 12.2* located on Cisco.com and the Documentation CD-ROM.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback or go to the following URL to give us your feedback:
http://forums.cisco.com/eforum/servlet/viewsflash?cmd=showform&pollid=rtgdoc01!rtgdoc.

Contents

These release notes describe the following topics:

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(8)YW3 and includes the following sections:

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YW3

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	Gateway GPRS Support Node Standard Feature Set	Gateway GPRS Support Node (GGSN) DES	c7200-g6ik8s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g6ik9s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g6is-mz	48MB	512MB	RAM

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YW2

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	Gateway GPRS Support Node Standard Feature Set	Gateway GPRS Support Node (GGSN) DES	c7200-g6ik8s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g6ik9s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g6is-mz	48MB	512MB	RAM

Table 3 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YW1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	Gateway GPRS Support Node Standard Feature Set	Gateway GPRS Support Node (GGSN) DES	c7200-g6ik8s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g6ik9s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g6is-mz	48MB	512MB	RAM

Table 4 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YW

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	Gateway GPRS Support Node Standard Feature Set	Gateway GPRS Support Node (GGSN) DES	c7200-g6ik8s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g6ik9s-mz	48MB	512MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g6is-mz	48MB	512MB	RAM

Supported Hardware

Cisco IOS Release 12.2(8)YW3 supports the following Cisco 7000 family platforms:

- Cisco 7200 NPE400 series routers with 512M

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 5.

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:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 YW Software (c7200-g6is-mz), Version 12.2(8)YW3, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to S*oftware Installation and Upgrade Procedures* located at the following URL:

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

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.2 YW supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2 YW can include new features supported by the Cisco 7000 family.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States 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 United States government regulations. When applicable, purchaser and 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.

Table 5 lists the features and feature sets supported by the Cisco 7000 family in Cisco IOS Release 12.2(8)YW3 and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, (8)YW means a feature was introduced in 12.2(8)YW. If a cell in this column is empty, the feature was included in the initial base release.

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com.

Table 5 Feature List by Feature Set for the Cisco 7200 Series

Features	In	Software Images by Feature Sets			
		Gateway GPRS Support Node (GGSN) DES	Gateway GPRS Support Node (GGSN) 3DES	Gateway GPRS Support Node (GGSN)	
GGSN 4.0	(8)YW	Yes	Yes	Yes	

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW3.

New Hardware Features in Cisco IOS Release 12.2(8)YW3

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW3.

New Software Features in Cisco IOS Release 12.2(8)YW3

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW3.

New Hardware Features in Cisco IOS Release 12.2(8)YW2

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW2.

New Software Features in Cisco IOS Release 12.2(8)YW2

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW2.

New Hardware Features in Cisco IOS Release 12.2(8)YW1

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW1.

New Software Features in Cisco IOS Release 12.2(8)YW1

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW1.

New Hardware Features in Cisco IOS Release 12.2(8)YW

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW.

New Software Features in Cisco IOS Release 12.2(8)YW

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YW:

GGSN 4.0

Platforms: Cisco 7200 series routers

GPRS 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.

The GGSN R4.0 release provide the combined 2.5G and 3G packet gateway support and interworking capability on the same node.

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 6.

Table 6 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
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

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2 YW that can apply to the Cisco 7000 family.

New Implementations and Behavior Changes in Cisco IOS Release 12.2(8)YW1

The following sections describe new implementations and behavior changes since the last release of the Cisco IOS GGSN software.

GTP Related Changes

The following new GTP related changes have been added to this release:

- GGSN allows GTP v0 PDP context create requests over an existing GTP v1 PDP context and vice-versa.
- GGSN drops update requests with a different version than the SGSN that currently owns the PDP context.

PPP Related Changes

The following PPP related changes have been added to this release:

- In this release, GGSN supports the LCP ACFC option for GTP PPP, in which the header (0xFF03) will be always stripped off for downlink PPP TPDUs. However, if the GGSN receives the first PPP TPDU with 0xFF03 from the SGSN, it will not strip off 0xFF03 for downlink PPP TPDU.
- In previous releases, the Reordering IE was always not set or set to ‘0’ in the Create PDP Context Response returned by a Cisco GGSN. With this release, in case of PPP PDP, it is always set. In case of IP PDP, it depends on the QoS profile.
- With this implementation on the GGSN, uplink TPDUs arriving at the GGSN that are in-sequence are processed and routed. Out-of-sequence TPDUs are dropped. No packet buffering and reordering will actually be done. Such sequencing is always performed on PPP PDP contexts or IP PDP contexts that have the delivery order set in the R99 QoS profiles.
- Previously, when PPP-regeneration was used, a user might be connected to a different domain other than the APN the user was connecting to. This is because when the protocol configuration option (PCO) IE of a create PDP context request contained a composite username (for example, user@domain), the GGSN would create a L2TP tunnel to this user to the domain specified in PCO IE. The GGSN did not validate this domain against the APN sent out by the user. The GGSN also selected an L2TP tunnel either using an APN name or the user-supplied domain name, and would always prioritize the user-supplied domain-name over the APN name. Therefore, regardless of the APN the user is connecting to, the GGSN would connect the user to the requested domain-name, using the L2TP tunnel for that domain.

- To enable bypassing this behavior, in this release a new access-point configuration command is supported.
- To configure for the GGSN to check the domain sent in the PCO IE with the APN, issue the following command in access-point configuration mode:

  ppp-regeneration verify-domain

Note If there is a mismatch, the create request would be rejected with the cause value “Service not supported”.

Charging Related Changes

The following new Charging related changes have been added to this release:

- When all charging gateways (CGs) are down, CDRs generated due to volume triggers, QoS, tariff, SGSN changes and forced partial CDR closures, as well as new PDP create/deletes, are buffered in GGSN processor memory. If the CGs are not brought up soon enough, this will eventually cause all the GGSN processor memory to be used up. Once this condition is reached, there will be no connectivity to the Cisco GGSN, through the console or any other IP connectivity. In addition, other IOS applications running on the router might have unpredictable behavior.

  To prevent the GGSN from completely draining out the processor memory because of abnormal conditions, such as the CGs being down, in this release the GGSN can be configured to do the following when this condition exists:

  – Reject new PDP create requests with cause value “No Resource Available”

  – Handle the following charging triggers and drop the PDP:

  a. Volume limits triggers that have occurred due to ongoing traffic on existing PDPs.

  b. QoS changes

  c. SGSN changes

  To enable this memory overload protection feature, issue the following command while in global configuration mode:

  gprs memory threshold <*x*>

- If the previous release, if the CG is perceived as being down by GGSN due to link failures, GGSN will not talk to the CG unless a node-alive is received from the CG. Some CGs can not send echo request, it is not able to detect the link failure and will not send node-alive, There would be no way GGSN can automatically recover from this failure.

  In this release, GGSN will periodically try to reconnect to the CG to detect if the link is up by sending echo request messages to the CG.

  To enable this feature, issue the following command while in global configuration mode:

  gprs charging reconnect <*minutes*>

Note The reconnect feature is enabled by the CLI only when UDP is used as the charging path protocol.

- In previous releases, if a data record transfer request message was retransmitted because it was not successfully acknowledged, the command IE had a value of "1" for "Send data record transfer packet," instead of "2" for "send possibly duplicated data record transfer packet." According to the specifications, the value of 1 should be only for unique messages. To mark the retransmission of unacknowledged messages with a command IE of "2," issue the following hidden command while in global configuration mode:

  gprs charging message transfer-request command-ie send-p

APN Related Changes

The following new APN related changes have been added to this release:

- To allow the configuration of the DNS/NBNS address at the APN level, the following two commands are supported in this release:

  dns primary <*address*> secondary <*address*>

  nbns primary <*address*> secondary <*address*>

  So now, the DNS and NBNS addresses to be sent to the MS can come from the following three sources:

  – DHCP Server

  – Radius Server

  – Local APN level configuration in GGSN

  The criteria for selecting the DNS/NBSN servers depend on the IP address allocation scheme specified under the APN. Specifically, the criteria are as follows:

  – For the DHCP-based scheme (both local & external), the one returned from the DHCP server is sent to MS. If the DHCP server does not return those addresses, then the local APN configuration is used.

  – For the RADIUS-based scheme, the one returned from the RADIUS server (in Access-Accept) is used. If the RADIUS server does not return those addresses, then the local APN configuration is used.

  – For the Local IP Address Pool-based scheme, the APN configuration is always used.

  – In the case of a static IP address, the local APN configuration will be used to select the DNS and NBNS address.

Note In all of the above cases, GGSN will send DNS and NBNS addresses in the create PDP response only if the MS is asking for those addresses in the PCO field.

Benefits of the APN level DNS/NBNS configuration include the following:

– For some address allocation schemes, like Local IP Address Pool, currently there is no mechanism to obtain these addresses.

– For a RADIUS-based allocation scheme, this configuration might be useful because the operator might prefer to configure these addresses under the APN rather than configuring under each of the user profiles.

- A new option is now supported that allows a configuring a local IP address pool under the APN to avoid using the DHCP proxy client interface. The following is a configuration example of how to use the local IP local address pool:

```
ip local pool my_local_pool 128.1.0.1 128.1.255.254
!
access-point 1
access-point-name cisco.com
ip-address-pool local my_local_pool
aggregate 128.1.0.0/16
exit
```

Security Related Change

The following new Security related changes have been added to this release:

- Previously, if a GGSN received an all zeroes (16 octets) CHAP challenge in the PCO IE in a GTP PDP context create packet, the GGSN replaced the CHAP challenge by a random value instead of forwarding it unchanged to the Request Authenticator field in the RADIUS Access-Request packet. Because the Request Authenticator is an input value for the MD5 hash function in the RADIUS server, the RADIUS authentication will fail with an Access-Reject. Any non-zero CHAP challenge will work correctly.

  In this release, the gprs radius attribute chap-challenge command has been introduced to fix this condition.

  To configure for the CHAP challenge to always be sent in the challenge attribute (and not in the authenticator field) in an Access-Request message to the RADIUS server, issue the following command while in global configuration mode:

  [no] gprs radius attribute chap-challenge

Behavior Changes in Cisco IOS Release 12.2(8)YW

1. Configure change for GTP virtual template:

   Previous configuration for GTP virtual template

```
!interface virtual-template1
  ip address 21.1.1.1 255.255.255.0
  encapsulation gtp
  gprs access-point-list gprs
!
```

   Recommended configuration for GTP virtual template

```
!interface loopback1
 ip address 21.1.1.1 255.255.255.255
!
interface virtual-template1
  ip unnumbered loopback1
  encapsulation gtp
  gprs access-point-list gprs
```

The recommended configuration unnumbers GTP's virtual template to a loopback interface on which the IP address is configured. On a loopback interface a single IP address, rather than a subnet of addresses, can be configured. It is a way to save up IP addresses. The previous configuration is still supported, but must be used with following command to avoid CEF switching problem for subinterfaces:

```
no vtemplate subinterface
```

2. New Attributes in Radius Messages

   The 3GPP Vendor Specific Attribute 3GPP- NSAPI is sent in all Radius messages.

3. Default Change for Charging Data Transfer Response Message

   Default for charging data transfer response message, IE 253 (Requests Responded Information Element), has changed from number responded to length.

   To switch back to the previous IE format of number responded, use following CLI:

   ```
   gprs charging message transfer- response number-responded
   ```

4. Default Change for Access Violation CLI under APN

   The previous syntax of "[no] access-violation [discard packet | deactivate-pdp-context]" is changed to "[no] access-violation deactivate-pdp-context"; that is, "discard packet" option is no longer supported. By default, if the command is not configured, the user packets are dropped.

Caveats for Cisco IOS Release 12.2 YW

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 12.2 and Cisco IOS Release 12.2 T are also in Cisco IOS Release 12.2(8)YW3.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*.

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 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 also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, **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/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Table 7 Caveats Reference for Cisco IOS Release 12.2 YW

DDTS Number	Open in Release	Resolved in Release
CSCdv69895		12.2(8)YW3
CSCdw28703	12.2(8)YW3	
CSCdw35157		12.2(8)YW3
CSCdw42791		12.2(8)YW3
CSCdw56516		12.2(8)YW3
CSCdw57035		12.2(8)YW3
CSCdx01088	12.2(8)YW	
CSCdx02283		12.2(8)YW2
CSCdx32495		12.2(8)YW3
CSCdx36197		12.2(8)YW3
CSCdx41392		12.2(8)YW3
CSCdx45096	12.2(8)YW	
CSCdx46375		12.2(8)YW3
CSCdx56743		12.2(8)YW3
CSCdx63927		12.2(8)YW1
CSCdx76632		12.2(8)YW3
CSCdx77088		12.2(8)YW2
CSCdx86464		12.2(8)YW3
CSCdy07908		12.2(8)YW1
CSCdy09519		12.2(8)YW3
CSCdy34494		12.2(8)YW3
CSCdy41412		12.2(8)YW3
CSCdy49341		12.2(8)YW3
CSCdy59547		12.2(8)YW1
CSCdy65242		12.2(8)YW1
CSCdy65416		12.2(8)YW1
CSCdy80552		12.2(8)YW3
CSCdy87641		12.2(8)YW1
CSCdz17155		12.2(8)YW3
CSCdz20676	12.2(8)YW3	
CSCdz25552	12.2(8)YW	
CSCdz32592	12.2(8)YW	
CSCdz33537		12.2(8)YW1
CSCdz39284		12.2(8)YW1
CSCdz41124		12.2(8)YW1
CSCdz52774		12.2(8)YW1

Table 7 Caveats Reference for Cisco IOS Release 12.2 YW (continued)

CSCdz55751		12.2(8)YW1
CSCdz60229		12.2(8)YW1
CSCdz61813		12.2(8)YW3
CSCdz71127		12.2(8)YW2
CSCdz73994		12.2(8)YW2
CSCdz82820		12.2(8)YW1
CSCdz83042		12.2(8)YW1
CSCdz83230		12.2(8)YW1
CSCdz87056		12.2(8)YW1
CSCdz89418		12.2(8)YW1
CSCea02355		12.2(8)YW1
CSCea03903		12.2(8)YW1
CSCea05529	12.2(8)YW1	
CSCea06252		12.2(8)YW1
CSCea12603		12.2(8)YW1
CSCea15645		12.2(8)YW1
CSCea16343		12.2(8)YW1
CSCea17365		12.2(8)YW1
CSCea19885		12.2(8)YW3
CSCea21438		12.2(8)YW1
CSCea22854		12.2(8)YW1
CSCea26072	12.2(8)YW1	
CSCea26882		12.2(8)YW1
CSCea27536		12.2(8)YW3
CSCea28282		12.2(8)YW1
CSCea28346		12.2(8)YW1
CSCea29085		12.2(8)YW1
CSCea29780		12.2(8)YW1
CSCea30807		12.2(8)YW2
CSCea31687		12.2(8)YW1
CSCea32240		12.2(8)YW3
CSCea33065		12.2(8)YW3
CSCea36231		12.2(8)YW3
CSCea40773		12.2(8)YW1
CSCea42294		12.2(8)YW2
CSCea46342		12.2(8)YW3
CSCea48261		12.2(8)YW1

Table 7 Caveats Reference for Cisco IOS Release 12.2 YW (continued)

CSCea49932		12.2(8)YW1
CSCea50731	12.2(8)YW1	
CSCea51030		12.2(8)YW3
CSCea51076		12.2(8)YW3
CSCea54851		12.2(8)YW3
CSCea56880		12.2(8)YW2
CSCea61583		12.2(8)YW1
CSCea61911		12.2(8)YW1
CSCea63657		12.2(8)YW1
CSCea67414		12.2(8)YW1
CSCea67422		12.2(8)YW1
CSCea70814		12.2(8)YW1
CSCea74777	12.2(8)YW1	
CSCea75343		12.2(8)YW3
CSCea80839	12.2(8)YW1	
CSCea80864		12.2(8)YW1
CSCea84750		12.2(8)YW1
CSCea89536	12.2(8)YW1	12.2(8)YW2
CSCea89654		12.2(8)YW2
CSCea91875		12.2(8)YW2
CSCeb02935		12.2(8)YW2
CSCeb06248		12.2(8)YW2
CSCeb09237	12.2(8)YW2	12.2(8)YW3
CSCeb10298		12.2(8)YW2
CSCeb10788		12.2(8)YW2
CSCeb13653		12.2(8)YW2
CSCeb14701		12.2(8)YW2
CSCeb26981		12.2(8)YW2
CSCeb30794		12.2(8)YW2
CSCeb32338		12.2(8)YW2
CSCeb34080		12.2(8)YW2
CSCeb37720		12.2(8)YW2
CSCeb39251		12.2(8)YW2
CSCeb40561		12.2(8)YW2
CSCeb42554		12.2(8)YW2, 12.2(8)YW3
CSCeb44447		12.2(8)YW2
CSCeb47381		12.2(8)YW3

Table 7 Caveats Reference for Cisco IOS Release 12.2 YW (continued)

CSCeb54680		12.2(8)YW3
CSCeb57842	12.2(8)YW3	
CSCeb68515	12.2(8)YW3	
CSCeb68994		12.2(8)YW3
CSCeb71522		12.2(8)YW3
CSCeb71963		12.2(8)YW3
CSCeb73365		12.2(8)YW3
CSCeb75798		12.2(8)YW3
CSCeb78836		12.2(8)YW3
CSCec00106		12.2(8)YW3
CSCec02651	12.2(8)YW3	
CSCec12828		12.2(8)YW3
CSCec14547		12.2(8)YW3
CSCec23697		12.2(8)YW3
CSCin07420		12.2(8)YW3
CSCin13431		12.2(8)YW1
CSCin22263	12.2(8)YW	
CSCin24118	12.2(8)YW	
CSCin24248		12.2(8)YW1
CSCin26358	12.2(8)YW	12.2(8)YW1
CSCin28922		12.2(8)YW3
CSCin29601		12.2(8)YW1
CSCin30772		12.2(8)YW1
CSCin31879		12.2(8)YW1
CSCin34191		12.2(8)YW1
CSCin34816		12.2(8)YW1
CSCin35416		12.2(8)YW1
CSCin35720		12.2(8)YW1
CSCin37030		12.2(8)YW1
CSCin37626		12.2(8)YW1
CSCin38469		12.2(8)YW1
CSCin39610	12.2(8)YW1	12.2(8)YW2
CSCin40107	12.2(8)YW3	
CSCin40563		12.2(8)YW1
CSCin41226	12.2(8)YW1	12.2(8)YW3
CSCin41417	12.2(8)YW1	12.2(8)YW2
CSCin41811		12.2(8)YW1

Table 7 Caveats Reference for Cisco IOS Release 12.2 YW (continued)

CSCin42763		12.2(8)YW1
CSCin42844		12.2(8)YW2
CSCin43269	12.2(8)YW1	
CSCin44260		12.2(8)YW2, 12.2(8)YW3
CSCin45222		12.2(8)YW3
CSCin45828		12.2(8)YW3
CSCin46406		12.2(8)YW2
CSCin46520		12.2(8)YW3
CSCin46829		12.2(8)YW3
CSCin46941		12.2(8)YW3
CSCin47452		12.2(8)YW2
CSCin48184		12.2(8)YW3
CSCin48375	12.2(8)YW2	
CSCin49460		12.2(8)YW3
CSCin49962		12.2(8)YW3
CSCin51533		12.2(8)YW3
CSCin51981	12.2(8)YW3	
CSCin52065	12.2(8)YW3	
CSCin53181		12.2(8)YW3
CSCin53566		12.2(8)YW3
CSCin56377		12.2(8)YW3
CSCin57809	12.2(8)YW3	

Open Caveats—Cisco IOS Release 12.2(8)YW3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YW3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw28703

  [Severity: 3]

  Internet Control Message Protocol (ICMP) host-unreachable messages are not sent for packets that are forwarded to a virtual interface when Cisco Express Forwarding (CEF) is enabled.

  This problem is observed on a Cisco 7500 series.

  Workaround: Disable CEF.

- CSCdz20676

  [Severity: 3]

  When a PPP type PDP context is created on a Cisco router running Gateway GPRS Support node, the accounting information as well as charging data is wrong for upstream traffic.

  There are no workarounds.

- CSCeb57842

  [Severity: 3]

  When very high rate of OPEN/CLOSE IP PDP, free process memory may drop below the memory threshold configured on GGSN. show proc cpu will show that PDP cleanup proc is taking nearly 100% of CPU. Meanwhile PDPs can not be cleaned up. “sh logging” will show a lot of these error messages:

  ```
  "
  Jul 10 04:52:15.707: gprs_free_pdp_inline: PDP 0x2626CEC0 with wrongRefCount 0x1
  Charging reserved 1
  Jul 10 04:52:15.707: gprs_free_pdp_inline: PDP 0x2626CEC0 with wrongRefCount 0x1
  Charging reserved 1
  "
  ```

  If GGSN is not overstressed, this issue will not happen.

  There are no known workarounds.

- CSCeb68515

  [Severity: 3]

  When high rate PPP PDP are activated/deactivated on GGSN with local DHCP server configured on GGSN to assign IP addresses, there is mismatch of number of open PPP PDP and number of DHCP IP addresses lease after all PDP are deleted

  Workaround: Use external DHCP server or use local pool on GGSN.

- CSCec02651

  [Severity: 3]

  Cisco GGSN does not send teardown indicator set when the DHCP address lease is expired and can not be extended. Hence in the condition where primary and secondary PDP’s are existing for the same IMSI there it might end up having the IP address released back to the DHCP server despite having at least one PDP still using the same.

  There are no known workarounds.

- CSCin40107

  [Severity: 3]

  On a Cisco Router running Gateway GPRS Support Node (GGSN) 12.2(8)YY2 image, CG redirection might fail when reconnect timeout is set to a low value.

  This will happen, in case we send a redirection request and the reconnect timeout is set to a low value e.g.: 1 min. Since reconnect echos are sent out after the expiry of the reconnect timer, if the cg which sent the redirection request has not gone down till that time, it will result in that CG becoming the active CG again and cg redirection will fail.

  Workaround: Set a very high value for reconnect timeout, which would make sure that the CG which sent the redirection request has gone down by the time the reconnect timer expires.

- CSCin51981

  [Severity: 3]

  CISCO GGSN runs out of IO memory and CPU will be hogged by GTP PDP Cleanup process when delete requests are sent to those pdps which are under process of deletion by some other means such as deactivation of pdps while access-violation happens.This problem occurs only if this scenario runs for multiple sessions and long hours.

  There are no known workarounds.

- CSCin52065

  [Severity: 3]

  When PPP PDP ACFC (i.e. no 0xFF03), for upstream traffic, if they are rejected due to the access-list configuration at the GGSN, we could see the traceback.

  There are no known workarounds.

- CSCin57809

  [Severity: 3]

  On CISCO GGSN,US byte counts rcv_byte_count/cef_up_byte are not incremented properly when cef is on incase off ppp term. session.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(8)YW3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YW3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv69895

  [Severity: 3]

  A router may experience a bus error at PC 0x60255024, address 0xD0D0D85.

  The problem occurs in normal production if a an As5300 running 5300 Software (C5300-IS-M), Version 12.1(8)AA is used.

  There are no workarounds.

- CSCdw35157

  [Severity: 2]

  Defining the AAA Server group display the following message after a power cycle:

  ```
  %RADIUS-3-SOURCEPORTALLOCERROR: Warning: Unable to allocate port 21645
  ```

  There are no known workarounds.

- CSCdw42791

  [Severity: 2]

  Multichassis Multilink PPP (MMP) Media Gateway Control Protocol (MGCP) calls do not work because of authentication failures.

  This problem is observed on a Cisco AS5400.

  Workaround: Use local authentication by enabling the **aaa authentication ppp default local** global configuration command.

  Alternate workaround: If RADIUS authentication is used, omit the “class” attribute from the RADIUS user profile.

- CSCdw56516

  [Severity: 3]

  Packets getting tunneled will not be ipsec-encrypted when physical interface, carrying tunneled packets, is configured to encrypt tunneled packets. This behavior is observed when Tunnel interface has no crypto configuration in it.

  There are no known workarounds.

- CSCdw57035

  [Severity: 2]

  The record of IPsec tunnel entries in the IKE stream are leaked when the IKE stream is destroyed. Under all conditions, a small piece of memory is leaked when an IKE Stream is destroyed.

  Workaround: Clear the IPsec tunnel list before freeing the IKE stream.

- CSCdx32495

  [Severity: 3]

  A Cisco router configured with crypto might reload.

  There are no known workarounds.

- CSCdx36197

  [Severity: 2]

  An SNMP enabled router could reload if the following sequence of events were to occur:

  1. An IKE SA dies or is otherwise killed

  2. An SNMP request comes in to list the active IKE tunnels.

  Knowledge of the SNMP community string is equivalent to the knowledge of the access and enable passwords to the router.

  When enabling SNMP on a router like with telnet or SSH access to the router care needs to be taken to only allow access from trusted hosts by using SNMP views and ACLs along with uRPF.

  Workaround: Disable SNMP or the view of the IPsec MIB.

  ```
  snmp-server view qwerty internet included
  snmp-server view qwerty cipSecMibLevel excluded
  snmp-server view qwerty ciscoIpSecFlowMonitorMIB excluded
  snmp-server view qwerty ciscoIpSecPolMapMIB excluded
  ```

- CSCdx41392

  [Severity: 1]

  The COPS MIBs code is being removed from the IOS code base as this feature is not currently supported. The files containing the code implementation of these MIBs have been commented out of the platform specific makesubsys.rsp / makesubsys.common files to resolved this issue.

  There are no known workarounds.

- CSCdx46375

  [Severity: 1]

  An as5400 might experience a crash when subjected to stress test in which calls are cleared from the client side for a certain period.

  The same reload may also be observed on Cisco router running Gateway GPRS Support Node IOS software

  There are no known workarounds.

- CSCdx56743

  [Severity: 2]

  A RADIUS attribute 69 that has special characters defined may fail in decryption.

  This problem is observed on a Cisco AS5400 that is running Cisco IOS Release 12.2(02)XB05 and may also be observed on 7200 series router running GGSN Image.

  There are no known workarounds.

- CSCdx76632

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCdx86464

  [Severity: 3]

  One a Cisco router acting as a L2TP Network Server, LCP may renegotiate when a PPP client requests no options. This may cause interoperability problems with clients who cannot handle LCP renegotiations.

  There are no known workarounds.

- CSCdy09519

  [Severity: 1]

  On a Cisco router, there is a possibility of router reload during IPSec tunnel teardown operation. This is a rare situation.

  There are no known workarounds.

- CSCdy33860

  [Severity: 2]

  Layer 2 Tunnel Protocol (L2TP) sessions are not established when the **vpn service** *domain-name* VC class configuration command is configured on the L2TP access concentrator (LAC) to authorize incoming PPP over Ethernet (PPPoE) clients.

  This problem is observed when an L2TP network server (LNS) uses a Cisco IOS image that has the fix for CSCdx86464.

  Workaround: Unconfigure the **vpn service** *domain-name* VC class configuration command on the LAC, and configure proxy Link Control Protocol (LCP) negotiation between the client and the LAC.

- CSCdy34494

  [Severity: 3]

  Nas-Identifier value is not correct due to which it only takes 33 char.

  There are no known workarounds.

- CSCdy41412

  [Severity: 2]

  A Cisco IOS router that is running a Data Encryption Standard (DES) or Triple DES (3DES) image may fail to establish tunnels, and the source address mask in the encryption access control lists (ACLs) for one or more tunnels may become corrupt.

  These problems are observed on a Cisco router that is running a DES or 3DES image of Cisco IOS Release 12.1(11b)E to Release 12.1(11b)E8 or Release 12.1(12c)E to Release 12.1(12c)E4 after the router has been running for some time and soon after one or more IP Security (IPSec) tunnels have been re-keyed. The symptoms may also occur in Release 12.2 T.

  For Release 12.1 E, Cisco recommends the following software upgrades:

  – For all Cisco 7100 series images, upgrade to Release 12.1(12c)E6.

  – For all Cisco 7200 series “-k2” and “-561” images, upgrade to Release 12.1 (12c)E6.

  The fix for this caveat has also been integrated in Release 12.2(15)T.

  There are no known workarounds.

- CSCdy49341

  [Severity: 3]

  On a Cisco router running IPSec image and using IPSec MIB, there might a possibility of memory held by IPSec MIB to increase as the Tunnel tables are created and deleted. This is not a memory leak but however the memory held by the IPSec MIB is not released immediately. This occurs when the tunnel tables are created and deleted often.

  There are no known workarounds.

- CSCdy80552

  [Severity: 2]

  A memory leak in the ISDN process may cause a Cisco AS5xxx voice gateway that is operating under stress conditions to reload.

  This problem is observed when more than one host that uses the Simple Network Management Protocol version 1 (SNMPv1) security model is configured on the router by entering the **snmp-server host** *host-addr* global configuration command such as in the following configuration:

  ```
  snmp-server host 10.30.50.41
  snmp-server host 10.30.50.40
  ```

  Workaround: Remove the multiple instances of configured SNMPv1 hosts. Only one host should be specified in the running configuration by entering the **snmp-server host** *host-addr* global configuration command.

- CSCdz17155

  [Severity: 3]

  The problem happens when several RADIUS servers configured.

  The problem occurs when the first two servers change there state from “DEAD” to “UP” within configured deadtime.

  There are no known workarounds.

- CSCdz61813

  [Severity: 3]

  On a Cisco router, when an interrupt hang condition is detected, the system reloads and no crashinfo is generated. crashinfo would give useful information and needs to be collected for this case. This occurs when a cisco router reloads due to an error interrupt.

  This is a rare situation where an error interrupt occurs on the Cisco router causing a reload. If such a case happens, Crashinfo is not generated.

  There are no known workarounds.

- CSCea19885

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea27536

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea32240

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea33065

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea36231

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea46342

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea51030

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea51076

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea54851

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCea75343

  [Severity: 3]

  In Cisco IOS Release 12.3(0.5), AAA requests sent to a server will not be encrpyted/decrypted, if the server group that a server belongs to is configured before the server is declared in the global server list.

  The following sequence of command will cause this problem to occur:

  1) Configure a Radius/Tacacs+ server group

  ```
  aaa group server radius rad-sg
   server 10.1.1.1 auth-port 1645 acct-port 1646
  !
  ```

  2) Configure the server in the global server list

  ```
  radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123.
  ```

  Send a aaa request.

  ```
  'debug radius' shows the following error messages:

  18:45:51: RADIUS: No secret to encode request (rctx:0x64C22B44)
  18:45:51: RADIUS: Unable to encrypt (rctx:0x64C22B44)

  18:45:51: RADIUS:  authenticator B8 61 52 46 5C 65 EE 9A - 81 33 93 46 FD E0 E6 21
  radius_decrypt: null length
  18:45:51: RADIUS: Response (54) failed decrypt
  ```

Workaround: Configure a global server key:

```
radius-server key rad123
```

Alternative workaround: Perform configuration in the reverse order:

1. Configure the global AAA server
2. Configure the AAA server group

- CSCeb09237

  [Severity: 3]

  On a Cisco router running Gateway GPRS support node software (GGSN), when PPP L2TP gtpv1 PDP contexts are created at a high rate and simultaneously deleted and if this repeated for a extended duration of time, the counter “gtp’s ppp va hwidbs” hits the value 8000 and causes GGSN to reject all further PPP PDP requests. The PDPs are not existent on GGSN although this counter shows 8000.

  This problem is observed on a 7200 Cisco router running 122-8YW image with the GGSN service enabled and create and delete PDP request is sent over a few thousand PDP contexts at a high rate for an extended period of time.

  There are no known workarounds.

- CSCeb42554

  [Severity: 3]

  A Cisco router running Gateway GPRS Support (GGSN) IOS software may leak small IO memory buffers.

  This happens only when UDP is configured as Charging protocol, the gprs charging reconnect feature is enabled and the leak happens when a CG goes down.

  Workaround: Most users should not use charging reconnect feature unless the CG does not support echo request. There is no leak if CG are up. Also the leak rate is one per reconnect echo.

- CSCeb47381

  [Severity: 5]

  When PDP create is rejected due to low memory, the error message “Num of PDP reaches limit”. It should be able to tell more specific reason for the rejection, i.e. lack of memory. This occurs under stressful conditions.

  There are no known workarounds.

- CSCeb54680

  [Severity: 3]

  If activate/deactivate PPP PDP for L2TP at the high rate with high traffic and charging on, there is some potential small memory leak on VPDN

  There are no known workarounds.

- CSCeb68994

  [Severity: 3]

  GGSN sends a wrong length in GTPv1 response message when the cause value is other than Request Accepted. The receiver would see some unwanted octets appended to the end of the packet.

  There are no known workarounds.

- CSCeb71522

  [Severity: 4]

  PDP context will not be created with cause of duplicate IP address used by MS.

  With some mobile to create a PDP context, IPCP some how get into address renegotiation and it caused error of duplicate IP address used by the MS to access the same APN.

  There are no known workarounds.

- CSCeb71963

  [Severity: 3]

  On a Cisco router running Gateway GPRS support node (GGSN) software, there is a possibility of processor memory fragmentation after repeated create requests are received at a high rate with protocol configuration options.

  The incoming create requests are received at a high rate and contains the protocol configuration options.

  There are no known workarounds.

- CSCeb73365

  [Severity: 3]

  A Cisco router running Gateway GPRS Support node software (GGSN) may reload with a corrupted program counter after displaying out of memory message. This is rare situation and may happen only when the router is running under stress conditions and no memory is available.

  The recommended gprs memory threshold is 512 (GGSN starts dropping PDPs when there 50MB left).

  Workaround: Disable charging or configure memory protection on the GGSN.

- CSCeb75798

  [Severity: 4]

  APNSelectionMode in partial CDR is zero.

  This problem occurs when “gprs charging cdr-option apn-selection-mode” is configured.

  There are no known workarounds.

- CSCeb78836

  [Severity: 1]

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks. This advisory is available at:

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml .

- CSCec00106

  [Severity: 3]

  GGSN reloads if charging redirection request is sent from a charging gateway with a very large length value in the Information Element (instead of the correct value of 4 for IPv4 types).

  There are no known workarounds.

- CSCec12828

  [Severity: 3]

  Cisco GGSN running Rel 3.1 or Rel 4.0 software, uses code 02 (CONF ACK) instead of 03 (CONF NACK) when sending back IPCP address related option(s) (IPCP address, primary/secondary DNS/NBNS address) in the PCO of Create PDP Context Response message even though the address(es) in the response message is/are different from that in the PCO of Create PDP Request message.

  There are no known workarounds.

- CSCec14547

  [Severity: 4]

  For a v1 PDP with a r99 QoS (QoS profile length 11), a change in the allocation/retention priority causes a container/CDR to be added.

  Normally this should not occur as a MS using a r99 QoS would not change its allocation/retention priority because it does not use it.

  There are no known workarounds.

- CSCec23697

  [Severity: 3]

  When a ISRAU is received with a different QoS, the first container in the second CDR repeats the byte counts that have already been reported in the last container of the previous CDR. The total byte counts for closing the CDR on volume trigger is still correct. This occurs when v1 PDP is updated with both SGSN and QoS at the same time.

  There are no known workarounds.

- CSCin07420

  [Severity: 3]

  Cisco GGSN running Rel 3.0 or Rel 4.0 software, accepts invalid IP addresses (e.g. 0.0.0.0, 127.0.0.1) as part of “aggregate ...” (under APN submode) and “gprs default aggregate ...” (global) configurations.

  There are no known workarounds.

- CSCin28922

  [Severity: 2]

  Accounting records are dropped if the encryption fails for the radius server. It would not get retried not try other servers.

  This problem was found on Cisco IOS 7200 platform and if radius encryption fails for an accounting request being to the first server in the list. The failure to encrypt may be due to incorrect secret.

  There are no known workarounds.

- CSCin41226

  [Severity: 3]

  Cisco GGSN may drop uplink packets for PPP PDP type when the Gi is configured under VRF. This happens when CEF is turned on.

  This happens for the following:

  – PPP PDP type,

  – When CEF is turned on

  – When the Gi interface is under VRF

  There are no known workarounds.

- CSCin44260

  [Severity: 2]

  For Cisco GGSN running 12.2(8)YW release, when GGSN receives the Routing Area Update to change the SGSN data address, the downstream traffic for PPP PDP fails to reach the SGSN. Those traffic will be dropped.

  There are no known workarounds.

- CSCin45222

  [Severity: 3]

  Cisco router running Gateway GPRS Support Node (GGSN) software, there is a possibility of a router reload when an APN is unconfigured while the command **show gprs access-point** is being executed.

  This is a rare situation when the show command is stopped in the more prompt and apn is removed from another telnet session.

  There are no known workarounds.

- CSCin45828

  [Severity: 2]

  Cisco GGSN reboots when the DHCP lease renewal failure happens simultaneously with the receipt of a create PDP request with changed recovery IE.

  There are no known workarounds.

- CSCin46520

  [Severity: 3]

  GGSN reloaded while executing shGprsGtpPdpAll after deleting v0 regen pdps and while crt/upd/del are happening on v1 path. When this happened there was a big difference in the sessions showed by shGtpStatus(2193) and shVpdn(2617) on GGSN.

  There are no known workarounds.

- CSCin46829

  [Severity: 3]

  Cisco GGSN keeps the TCP connection to both the PRIMARY and Secondary CG as UP and in ESTAB state under stress scenario or when memory is low.

  There are no known workarounds.

- CSCin46941

  [Severity: 3]

  Cisco GGSN reloads while displaying the pdp using show gprs gtp pdp tid <> at the same time when pdps are deleted.

  There are no known workarounds.

- CSCin48184

  [Severity: 3]

  In Cisco 7200 series router running gateway gprs support node IOS software ppp-regen verify-domain feature does not work in case vpdn domain-delimiter is other than the default '@'

  Workaround: Wse the default vpdn domain-delimiter, which is “@”.

- CSCin49460

  [Severity: 3]

  When GGSN receives a re-create request (create PDP request on an existing PDP) for a PDP type of PPP, it deletes the PDP.

  This is observed only for PPP PDP type & for a re-create request (the original PPP PDP create request works fine).

  There are no known workarounds.

- CSCin49962

  [Severity: 3]

  Under stress condition with charging tariff time expiry and GGSN hits low memory threshold, PDP contexts may fail to be deleted.

  There are no known workarounds.

- CSCin51533

  [Severity: 3]

  GGSN rejects a GTP v1 create request for PPP PDP type if there’s already one existing. GTP v0 works fine in the same scenario.

  This problem is seen only for GTP v1 and for PPP PDP type.

  There are no known workarounds.

- CSCin53181

  [Severity: 3]

  A Cisco router running Gateway GPRS Support node software (GGSN), may reload due to access to an illegal address. This occurs when the process on the GGSN that is sending out a GTP response is suspended, due to multiple pending events. If any of these events acts on this PDP context causing its deletion within this timeframe, there is a possibility of a reload, if the suspended process accesses this context after resumption. This is an extremely rare situation.

  There are no known workarounds.

- CSCin53566

  [Severity: 2]

  GGSN crashes with the following traceback:

```
0x60798124:free(0x6079809c)+0x88
0x60024680:gtp_gtpsock_free(0x60024658)+0x28
0x60025CDC:gtp_io_cleanup_gtpsock(0x60025ca0)+0x3c
0x600263D8:gtp_io_process_message(0x600260ec)+0x2ec
0x60026850:gtp_io_process(0x60026704)+0x14c
```

  This crash happens in come images. It is a combination of events happening at the same time.

  There are no known workarounds.

- CSCin56377

  [Severity: 3]

  CDR is not closed when “gprs charging container sgsn-change-limit” in the GGSN is configured more than zero and sgsn change condition limit is hit.:

  1. Configure “gprs charging container sgsn-change-limit” as 1.

  2. Create a PDP context.

  3. Send two RA update requests.

  The expected behavior is to close the current CDR with the arrival of second RA update request but here this is not happening and no CDR is closed in the system.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(8)YW2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YW2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCeb09237

  [Severity: 3]

  On a Cisco router running Gateway GPRS support node software (GGSN), when PPP L2TP gtpv1 PDP contexts are created at a high rate and simultaneously deleted and if this repeated for a extended duration of time, the counter “gtp’s ppp va hwidbs” hits the value 8000 and causes GGSN to reject all further PPP PDP requests. The PDPs are not existent on GGSN although this counter shows 8000.

  This problem is observed on a 7200 Cisco router running 122-8YW image with the GGSN service enabled and create and delete PDP request is sent over a few thousand PDP contexts at a high rate for an extended period of time.

  There are no known workarounds.

- CSCin48375

  [Severity: 3]

  This problem is found to have happen to cisco GGSN Release R4.0 (12.2(8) YW2)

  The problem is that when there is a delay in create response for a radius req and in the mean time pdps are deleted ggsn could crash.

  There are no known workaround.

Resolved Caveats—Cisco IOS Release 12.2(8)YW2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YW2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx02283

  [Severity: 2]

  Router with a directly connected source does not register correctly with the RP over a gre tunnel.

  There are no known workarounds.

- CSCdx77088

  [Severity: 2]

  A software-forced reload may occur on a router, and the following messages may be displayed:

  ```
  System was restarted by error - a Software forced crash, PC 0x60396E7C at 4500
  Software (C4500-A3JS-M), Version 12.2(8.1), MAINTENANCE INTERIM SOFTWARE
  Compiled (current version) Image text-base: 0x60008948, data-base: 0x61116000
  Stack trace from system failure: FP: 0x618A8458, RA: 0x60396E7C FP: 0x618A8458,
  RA: 0x603952F4 FP: 0x618A8480, RA: 0x6039D584 FP: 0x618A84A0, RA: 0x603A0CC8
  FP: 0x618A84C0, RA: 0x60398BDC FP: 0x618A8558, RA: 0x6037E1F0 FP: 0x618A85A0,
  RA: 0x6174B1F0
  ```

  This problem is observed on a Cisco router that is running Cisco IOS Release 12.2(8.1)

  There are no known workarounds.

- CSCdz71127

  [Severity: 1]

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCdz73994

  [Severity: 3]

  In 12.2(8) or 12.2(13.7)T1 or later, RADIUS secret's of certain lengths may cause communication failure with the RADIUS server. For 12.2B, the known lengths which cause failures are 8 bytes and 20 bytes. For 12.2T it is 24 bytes.

  Workaround: Change the key length. An odd-numbered key length will always work.

- CSCea30807

  [Severity: 2]

  GGSN reloads due to I/O memory corruption under PPP PDP related stress condition when 8000 PPP PDP contexts were created and then deleted while downstream data were still being sent through them.

  There are no known workarounds.

- CSCea42294

  [Severity: 2]

  When signalling packets are continuously pumped to Gn while GGSN is being reloaded, the box may crash while it is booting.

  There are no known workarounds.

- CSCea56880

  [Severity: 2]

  Cisco GGSN R4.0 (IOS release 12.2(8)YW1) blocks downlink TPDUs for PPP PDP type when the Gi interface is under VRF & CEF is turned on.

  This happens only when all the following conditions are present:

  – PPP PDP type

  – Gi interface under VRF

  – CEF is turned on

  There are no known workarounds.

- CSCea89536

  [Severity: 3]

  Cisco GGSN shows high CPU utilization when there are a lot of PDPs pending for address allocation and SGSN starts sending the same create PDP request with different sequence numbers.

  There are no known workarounds.

- CSCea89654

  [Severity: 4]

  This is not really a bug, but an unclarity in the output of the show gprs gtp pdp-entry command. When L2TP is used with any PPP PDP contexts, this show output will display their MS addresses as Pending, even after the L2TP and PPP session has been up on them already.

  There are no known workarounds.

- CSCea91875

  [Severity: 3]

  Currently, PPP regeneration does not support a vpdn domain-delimiter other than the default '@'.

  This ddts add the support for non-default vpdn domain-delimiters, using the global configuration command **vpdn domain-delimiter**.

  There are no known workarounds.

- CSCeb02935

  [Severity: 3]

  IO memory leak during CDR transfer.

  Even though this problem is found when Charging is configured with small queue size and send buffer size. This could happen in any configuration, but with less chance to reproduce.

  Workaround: Using normal charging configg related to CDR transfer should reduce the chance of this leak.

- CSCeb06248

  [Severity: 2]

  A Cisco router running Gateway GPRS Support node software (GGSN), may reload under stress conditions with PPP PDP type contexts active on the GGSN. This is a rare situation when PPP link goes down and GGSN needs to send out delete requests informing SGSN to delete the PDP. If GGSN is under load and not able to send these delete requests immediately, but instead keeps these pending requests to send later, and meanwhile a SGSN change PDP update request is received which results in PDP context parameters updated. Later the GGSN may reload if the delete request is retried to send out.

  This is an extremely rare situation and happens only if the box is stressed for a long time.

  There are no known workarounds.

- CSCeb10298

  [Severity: 3]

  A Cisco router running gateway GPRS Support node software does not add route to MS when framed-netmask attribute is zero or not returned by radius server or when dhcp returns without a netmask.

  There are no known workarounds.

- CSCeb10788

  [Severity: 2]

  There are cases where IOS DHCP client reuses the ip lease information for another new address request; but at this point it does not update the client context. Because of this, the router might reload in some cases.

  There are no known workarounds.

- CSCeb13653

  [Severity: 3]

  GTPv1 Network-initiated PDP activation fails because the PDU Notification Request GGSN sends is missing the PDP address in End User Address IE.

  There are no known workarounds.

- CSCeb14701

  [Severity: 3]

  Cisco GGSN reloads when there is a delay in getting the DHCP response and in the mean time PDP is deleted.

  There are no known workarounds.

- CSCeb26981

  [Severity: 2]

  Cisco GGSN reloads when the **clear gprs charging cdr all** command is issued.

  When PPP PDP w/L2TP creates and deletes over a long period of time. When all the signalling messages stop, and all PDP contexts have been deleted, the GGSN has some CDRs without PDP contexts

  There are no known workarounds.

- CSCeb30794

  [Severity: 2]

  On a Cisco router running Gateway GPRS Support node software (GGSN), there is a possibility of a router reload due to access to an illegal address. This is when GTP tries to send out a response message and during this time, the PDP context is cleared on GGSN.

  This is an extremely rare situation and one scenario where this happen is when GGSN initiates a PDP delete and before actual deletion a create is received. This problem cannot be recreated easily.

  There are no known workarounds.

- CSCeb32338

  [Severity: 4]

  Cisco GGSN incorrectly deletes the path to map convertor when a GSN is used as both SGSN and map convertor, in the following scenario:

  1. Configure map convertor when GGSN reloads. It creates a v1 path.

  2. SGSN then sends some v0 create requests. This now creates a v1 path.

  3. Start NIPDP, and let it fail.

  4. GGSN deletes the v1 path to map convertor.

  This happens only when a GSN is used as both SGSN and map convertor. Also, this is only a minor problem not affecting the functionality. A subsequent NIPDP request will cause path lookup to happen which will pull up the v0 path.

  There are no known workarounds.

- CSCeb34080

  [Severity: 2]

  Cisco GGSN reloads in some cases where the IP address lease issued by DHCP server is renewed successfully.

  There are no known workarounds.

- CSCeb37720

  [Severity: 3]

  When GGSN R4.0 receives an update for a pdp with a new SGSN address, the counters in **show gprs gtp status** may show incorrect values.

  There are no known workarounds.

- CSCeb39251

  [Severity: 2]

  This problem is found to have happened to Cisco GGSN Release 3.1 in 12.2(8)YY2 and 4.0 in 12.2(8)YW1.

  The problem is that when GTP receives a TPDU which inner IP payload is of an invalid length longer than what the GTP header length or the outer IP header length indicates, then IO memory corruption happens causing the GGSN to crash.

  There are no known workarounds.

- CSCeb40561

  [Severity: 2]

  On Cisco IOS 12.2(8) YW releases, the router may crash if the router is low on processor memory and SNMP get operations are done on OSPF MIBs.

  There are no known workarounds.

- CSCeb42554

  [Severity: 3]

  GGSN leaks small IO memory buffers.

  This happens only when UDP is configured as Charging protocol, the gprs charging reconnect feature is enabled and the leak happens when a CG goes down.

  Workaround: Most users should not use charging reconnect feature unless the CG does not support echo request. There is no leak if CG are up. Also the leak rate is one per reconnect echo.

- CSCeb44447

  [Severity: 2]

  GGSN may reload under stress condition of duplicate Dynamic (address allocation by DHCP) context create requests with RADIUS authentication coming at high rate.

  There are no known workarounds.

- CSCin39610

  [Severity: 3]

  Cisco GGSN is not including all the requested IPCP configuration options in the Create pdp response message incase if a Create request comes with unsupported IPCP option (compression info) along with the other supported options request.

  There are no known workarounds.

- CSCin41417

  [Severity: 3]

  CISCO GGSN Running R4.0 leaks I/O memory if a create/delete pdp context is received on an existing pdp the is awaiting Radius/Dhcp server response.

  This occurs only if the request is not a retry i.e it contains a different GTP sequence number from the earlier one and also if the GGSN is awaiting a response from Radius/DHCP for this context.

  There are no known workarounds.

- CSCin42844

  [Severity: 3]

  This problem happens to the redirection of mobile-to-mobile traffic in Cisco GGSN's YW Throttle Release 4.0. When such traffic is sent from any mobile to another which uses the PPP PDP type, during the redirection of this traffic away from the egress APN towards a Gi interface, the number of bytes in these redirected packets is accounted incorrectly on the GGSN. A few more bytes would be accounted and shown in the show output under the corresponding PDP context. This problem does not happen if the PDP type of the second mobile handset is not PPP.

  There are no known workarounds.

- CSCin44260

  [Severity: 2]

  For Cisco GGSN running 12.2(8)YW release, when GGSN receives the Routing Area Update to change the SGSN data address, the downstream traffic for PPP PDP fails to reach the SGSN. Those traffic will be dropped.

  There are no known workarounds.

- CSCin46406

  [Severity: 3]

  This problem happens to GPRS's display of PDP entries for its show commands. When the interface number of a GTP-created PPP vaccess has more than 3 digits, the MS Address field is not wide enough for printing the vaccess name out so that its display bumps into the Source field causing it to print out unexpected output.

  This problem occurs to GGSN Release R4.0 in 12.2(8)YW2 and has been corrected there already as well.

  There are no known workarounds.

- CSCin47452

  [Severity: 6]

  A Cisco router running Gateway GPRS Support node Software (GGSN) generates Charging Call Data Records (CDRs) even if there are no charging gateways configured. Charging is enabled by default and hence this can lead to CDR accumulation on GGSN decreasing the available processor memory. If CDR generation is not desired, and if Charging is not disabled and system is operational, GGSN has to be reloaded to disable CDR generation. This is a feature to disable CDR generation in case GGSN does not have any charging gateways configured.

  Workaround: GGSN has to be reloaded and charging needs to be disabled with the command **gprs charging disable** before GGSN is put into operation.

Open Caveats—Cisco IOS Release 12.2(8)YW1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCea05529

  A Cisco Router running Gateway GPRS Support node (GGSN) release 3.0 software may reload due to CLI "clear gprs gtp pdp all".

  There are no known workarounds.

- CSCea26072

  When a cisco router running gateway GPRS support node software (GGSN), receives a create request with a MS address that is the same as the Charging-gateway address, there is a possibility of the router reloading due to memory corruption.

  This problem occurs only when charging is enabled on GGSN and a MS address is the same as the charging gateway address.

  Workaround: Configure gprs plmn exclude-range for the CG address. This would cause the create request with this address to be rejected.

- CSCea50731

  When the virtual-template interface used for GT's PPP PDP contexts is configured with both CLIs "ppp lcp delay..." and "ppp direction callin" the LCP negotiation packets sent from any virtual-access interfaces cloned from it do not include the authentication method configured under it. Thus, the peers think that no authentication is necessary and then they skip right to the IPCP phase from the LCP phase. This problem happens to Cisco GGSN's Release 12.2(8)YW on Mar 1 2003.

  Workaround: Do not configure the CLI "ppp direction callin" on this virtual-template interface.

- CSCea74777

  Cisco GGSN stops sending Radius requests while the AAA Server group configuration is changed and there are already active sessions using that particular server group.

  There are no known workarounds.

- CSCea80839

  GGSN may reload if the IP local pool is unconfigured and then configured back while there exist a large number of PDP contexts with address allocated from the IP local pool and radius authentication, and delete requests for those PDPS are being sent at a high rate.

  There are no known workarounds.

- CSCea89536

  Cisco GGSN shows high CPU utilization when there are a lot of PDPs pending for address allocation and SGSN starts sending the same create PDP request with different sequence numbers.

  There are no known workarounds.

- CSCin39610

  Cisco GGSN is not including all the requested ipcp config options in the create response incase if a crt req comes with unsupported ipcp option (compression info) along with the other supported options request.

  There are no known workarounds.

- CSCin41226

  Cisco GGSN may drop uplink packets for PPP PDP type when the Gi is configured under VRF. This happens when CEF is turned on.

  This happens under the following conditions:

  – For PPP PDP type
  – When CEF is turned
  – When the Gi interface is under VRF

  There are no known workarounds.

- CSCin41417

  CISCO GGSN Running R4.0 leaks I/O memory if a create/delete pdp context is received on an existing pdp the is awaiting Radius/Dhcp server response.

  This occurs only if the request is not a retry i.e it contains a different GTP sequence number from the earlier one and also if the GGSN is awaiting a response from Radius/DHCP for this context.

  There are no known workarounds.

- CSCin43269

  A Cisco router running Gateway GPRS Service node software reloads when a SGSN address is the same as a CG address.

  Workaround: Have different IP addresses for CG and SGSN.

Resolved Caveats—Cisco IOS Release 12.2(8)YW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx63927

  A Cisco single-port Fast Ethernet 100BASE-TX port adaptor (PA-1FE) may cause a software-forced reload.

  This symptom has been observed on a Cisco 7200 series router. Other Cisco series routers that use a PA-1FE may also exhibit this symptom. This problem is a result of hitting a corner case. The likelihood of hitting a corner case increases with the number of interface resets.

  There are no known workarounds.

- CSCdy07908

  Authentication, authorization, and accounting (AAA) RADIUS is not updating MIB statistics that are used by the AAA-SERVER-MIB. Configuration information is updated properly, but the request statistics or sever state objects that are used by the AAA-SERVER-MIB are not updated.

  This symptom is observed on a Cisco router.

  There are no known workarounds.

- CSCdy59547

  When the radius-key is not configured, if GGSN receives a Create Request for non-transparent APN, it does not send back a response and the PDP entry (which is in pending state) will not be deleted (it can be cleared manually though).

  Workaround: This problem can be avoided if the radius key is properly configured.

- CSCdy65242

  When creating an access-point using VRF LOCAL DHCP server to allocate address, the VRF local DHCP server does not response to the DHCP discover message, so the address allocation fails.

  This problem only occurs when on the VRF local DHCP server.

  Workaround: The user can use the global local DHCP server shared by multiple VRFs.

- CSCdy65416

  When create access-point using VRF LOCAL DHCP server to allocate address, the VRF local DHCP server did not response the DHCP discover message, so the address allocation fails.

  This problem only occurs on the VRF local DHCP server.

  Workaround: Use global local DHCP server shared by multiple VRFs.

- CSCdy87641

  On a CISCO router running Gateway GPRS Support Node (GGSN) image, GGSN does not send response back using the source IP address given in the original signalling request as the Destination IP Address. It right now uses the SGSN address as the Destination IP address.

  According to Section 10.2.1.1 in the 29:060 Spec, GGSN should send a response to the SGSN using the source IP address given in the Original signalling request as the Destination IP Address.

  This happens only for the tunnel signalling messages like creates, deletes and updates and not for the path signalling messages like echo.

  There are no known workarounds.

- CSCdz33537

  When a Cisco router running Gateway GPRS support node (GGSN) software, acting as GDM receives a create request without the PCO IE, the create request is rejected. However the GDM should do DNS lookup based on the APN IE and load balance the create request.

  There are no known workarounds.

- CSCdz39284

  Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) “PROTOS” Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

  This issue is observed on Cisco devices which contain support for the SIP protocol and are running vulnerable versions of software.

  Workaround: Cisco will be making free software available to correct the problem as soon as possible. Additional workarounds will be documented in the Security Advisory.

  This advisory is available at the following URL
  http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml .

- CSCdz41124

  Multiple Cisco products contain vulnerabilities in the processing of Session Initiation Protocol (SIP) INVITE messages. These vulnerabilities were identified by the University of Oulu Secure Programming Group (OUSPG) “PROTOS” Test Suite for SIP and can be repeatedly exploited to produce a denial of service.

  This issue is observed on Cisco devices which contain support for the SIP protocol and are running vulnerable versions of software.

  Workaround: Cisco will be making free software available to correct the problem as soon as possible. Additional workarounds will be documented in the Security Advisory.

  This advisory is available at the following URL
  http://www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml .

- CSCdz52774

  Cisco 7200 Router running GGSN image (12.2(12)) may reload due to illegal access to a low address if a particular race condition occurs when a delete context request is received by GGSN even before a create response has been sent back by GGSN for a PDP context.

  This happens under the following specific race condition: After radius authentication and authorization are successful, but before sending back create response, the process gets suspended and, by chance, the pdp context gets deleted in a different process flow.

  There are no known workarounds.

- CSCdz55751

  If one access list is used by more than two APNs on GGSN, removing one of the APNs will cause that access list being deleted automatically in the running configuration. Those remaining APNs that use the same access list will see a new (usually 185404173) number replacing the original one in access-list related command.

  There are no known workarounds.

- CSCdz60229

  Cisco devices which run IOS software and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default.

  This symptom is observed on all Cisco devices running IOS and containing support for the Secure Shell (SSH) server.

  Workaround: Cisco will be making free software available to correct the problem as soon as possible.

  The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at the following URL

  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml .

- CSCdz82820

  GGSN Rel 4.0 reloads when multiple instances of test scenarios involving many GTP v0 PDP context create requests, delete requests, QoS update requests and sending T-PDUs are run. The following alignment error message appears during the reload:

  ```
  Illegal access to a low address
  ```

  There are no known workarounds.

- CSCdz83042

  If the GGSN receives an all zeroes (16 octets) CHAP challenge in the PCO Information Element in a GTP PDP Context Create Packet, the GGSN will replace the CHAP challenge by a random value instead of forwarding it unchanged to the Request Authenticator field in the RADIUS Access-Request packet. As the Request Authenticator is an input value for the MD5 hash function in the RADIUS server, the RADIUS authentication will fail with an Access-Reject. So far, this problem has only been seen with Nokia Mobile GPRS Devices. Any non-zero CHAP challenge will work correctly.

  This problem is fixed by introducing the following CLI:

  ```
  [no] gprs radius attribute chap-challenge
  ```

  If this is configured, the CHAP challenge will always be sent in the challenge attribute in an Access-Request message to the Radius server, and not in the authenticator field.

  There are no known workarounds.

- CSCdz83230

  The user has to config a static route or loopback interface in global address space that match the VRF DHCP local server address.

  There are no known workarounds.

- CSCdz87056

  Cisco router running with R4.0 image may reload when creating 180k sessions and clearing them.

  This may occur when creating 180k sessions with 90K as authenticated from radius server and ip address from DHCP server:

  ```
  Image c7200-g6is-mz.v122_8_yw_122002
  ```

  There are no known workarounds.

- CSCdz89418

  Cisco router running with GGSN R4.0 image shows extra parameter “Charging Time Limit” in the show gprs charging parameters.

  This is a cosmetic issue, and no affect on functionality.

  There are no known workarounds.

- CSCea02355

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

- CSCea03903

  This bug does not affect R99 behavior.

  The charging enum for QoS mean throughput change in 32.015 CR 034 should be only applied to release 99 “gprs charging release 99”.

  Similarly, 32.015 CR025 about making MS address in CDR absent for PPP PDP should also only apply to R99.

  This situation occurs when “gprs charging release 98” is configured.

  Workaround: Regard the value of 31 as 0 for the QoS mean throughput.

  Alternative workaround: Regard the ip address 0.0.0.0 as if it is not present.

- CSCea06252

  When all CGs are down, CDRs that are generated due to volume triggers, QoS, tariff, SGSN changes and forced partial CDR closures, as well as new PDP create/deletes, are buffered in GGSN process memory. This will eventually cause all memory to be used up if CGs are not brought up soon enough. Telnet to the box will not be possible if the current session has timed out. TCP connection used by CDR transfer cannot be reestablished and the GGSN can not be recovered. Other IOS applications running on the box may also have unpredictable behavior.

  To prevent GGSN from completely out of memory due abnormal conditions such as CG down, GGSN will stop processing Charging triggers when the memory runs dangerously low. The default threshold is 50MB. When this happens, GGSN will r eject new PDP create requests with cause value "no resource" and the following charging triggers will be ignored:

  - Volume limit triggers that have occurred due to ongoing traffic on existing PDPs.
  - QoS changes
  - Tariff changes
  - SGSN changes
  - Partial CDR closures issued from CLI

  Note, however, that the byte counts are still kept and will be reported after the GGSN recovers. Since some change conditions are not handled, some of the byte counts will not have the accurate charging condition, i.e. QoS and tariff. However there is no corruption in the CDRs and the CDRs conforms to all CDR encoding rules. It is just as if those triggers never happened.

  The Caveat here is that some CDRs will have incorrect charging condition due to the non-handling of tariff and QoS triggers.

  This problem occurs when the GGSN is in relatively high load, in terms of ongoing traffic, and PDP create/delete/udpates. All CG's are down and CDR can not be sent out.

  There are no known workarounds, but every measure should be taken to ensure that at least one CG is always up and connected to the GGSN via reliable network. Locally and directly connected CGs are highly recommended.

  The impact is some CDR containers will not have correct QoS and tariff time.

- CSCea12603

  In the 3GPP standard, GTP reordering is mandatory for the PPP PDP type. However, GTP reordering has not been supported on the Cisco GGSN due to the concern over its performance and realistic benefit. Therefore, the Reordering IE in GTP's Create PDP Context Response returned by a Cisco GGSN is always not set and such reordering is never implementing.

  But due to this mandatory requirement added to the standard by a previous CR, GTP sequencing is now implemented on the GGSN in Release 12.2(8)YW as a way to honor this requirement on reordering.

  With this implementation on the GGSN, uplink TPDUs arrived at the GGSN that are in-sequence will be processed and routed further. Out-of-sequence ones will be dropped. No packet buffering and reordering will actually be done. Such sequencing is always performed on PPP PDP contexts or IP PDP contexts that have the orderly delivery set in their R99 QoS profiles.

  There are no known workarounds.

- CSCea15645

  Cisco GGSN reloads upon receiving an address purge notification from DHCP server for an already deleted PDP.

  This is a corner case where GGSN sends an Address Release request for an address and simultaneously gets an address purge notification.

  There are no known workarounds.

- CSCea16343

  If a data record transfer request message is retransmitted because it was not successfully acknowledged, the command i.e. will have the value of "1" for "Send data record transfer packet", instead of "2" for "send possibly duplicated data record transfer packet". According to the spec, the value of 1 should be only for unique messages.

  This problem occurs when the **gprs charging message transfer-request command-ie** command is configured.

  There are no known workarounds.

- CSCea17365

  GGSN may experience high CPU utilization while processing delete pdp context requests when there are in excess of 150 thousand active PDPs.

  There are no known workarounds.

- CSCea21438

  This problem happens with the Cisco GGSN release 12.2(8)YW after the suppression of the PPP control and address fields is implemented. This problem occurs in a small window when a PPP PDP context is in the process of being deleted and data traffic is simultaneously received on it.

  Workaround: Turn CEF off, though this will cause the activation rate and throughput to drop significantly.

- CSCea22854

  The new **gprs watermark memory** command has some problems. When the **no gprs watermark memory** command is used or the default value of 512 is set, the running config would be saved wrongly with a value of "0", and the next time the GGSN is reloaded, it will have parser errors due to the fact that "0" is in the valid range.

  In addition, the **no gprs watermark memory** command does not work.

  This problem occurs after the running config is saved when the **gprs watermark memory 512** command is used.

  Workaround: Load a config without the **gprs watermark memory** command and do not save it.

- CSCea26882

  GTPv1 upstream T-PDU is corrupted when CEF is enabled and the GGSN is configured to ignore UDP checksum.

  There are no known workarounds.

- CSCea28282

  When a Cisco router running Gateway GPRS Support node software, receives a delete PDP request while the create is still being processed and an IP route is being added to this MS, there is a possibility of a reload.

  This problem occurs when IP route insertion process gets suspended and in the meantime the PDP is deleted.

  There are no known workarounds.

- CSCea28346

  It is possible for a Cisco GGSN to create more than 8000 PPP virtual-access interfaces for its PPP users, although 8000 is the maximum number that we can support. This usually happens when there is a delay or error in bringing PPP sessions down and the same users turn around to create the sessions again almost immediately.

  This resolution is to implement a check on the current number of such interfaces created, before GTP goes ahead to create more. If the current number reaches 8000 for the current release, GTP will reject the context creations. This resolution is implemented in 12.2(8)YW and later. So far, this limit is only hard-coded and not configurable.

  There are no known workarounds.

- CSCea29085

  In a Cisco router running Gateway GPRS Support node (GGSN) image, if the Charging Gateway gets down (or perceived down), GGSN currently will not try to reconnect to that CG to detect if the CG is up. If the CG does not send echo requests, it will not be able to detect the connection problem and therefore will not send node-alive. GGSN will stop trying to reconnect after it is unable to reach the CG.

  There are no known workarounds.

- CSCea29780

  Cisco GGSN may create 2 paths (as seen by “show gprs gtp path”) to the same SGSN under the following scenario:

  1. SGSN & GTP-MAP convertor (interface to HLR) have the same IP address.

  2. Link between SGSN/MAP-convertor & GGSN is down initially. At this point you configure “gprs default map-con <sgsn/map-convertor>. GGSN would try to establish a v1 path but since the link is down it would clear v1 path after N3 retransmissions of echoes and fall back to v0. Further, after N3 retransmissions on v0 path, it would eventually stop. But the path stays up.

  3. At this point, the link between SGSN/MAP-convertor & GGSN comes up. Now, SGSN sends a v1 create request. Since the version on v0 path is not confirmed, GGSN accepts this request. Now you have two paths.

  There are no known workarounds.

- CSCea31687

  A Cisco router running Gateway GPRS Support node (GGSN) and PPP-Regeneration feature is used, there is a possibility of user being connected to a different domain other than the APN, the user is connecting to.

  When the PCO options from the user, has a composite username i.e user@domain, then GGSN would proceed to create a L2TP tunnel to this user to the domain specified in PCO IE. GGSN does not validate this domain against the APN sent out by the user.

  There are no known workarounds.

- CSCea40773

  Number of maximum data SGSN addresses per signalling SGSN address is exceeded and new SGSN updates are rejected with SYSTEM_FAILURE (204)by the GGSN.

  This situation happens if the number of data SGSNs is exceeded. In this release it is 5.

  There are no known workarounds.

- CSCea48261

  Cisco GGSN does not ignore Guaranteed Bit Rate for Interactive and Background traffic class.

  There are no known workarounds.

- CSCea49932

  Cisco GGSN doesn't handle multiple GTP versions on the same path.

  If the version on a path to GSN is confirmed, GGSN drops subsequent messages of different GTP version received on the same path. GGSN confirms the version on a path when it receives a message of that version from its peer.

  There are no known workarounds.

- CSCea61583

  When pdp is to create in non-transparent APN, if the APN is configured to get address from local pool. When the local pool is exhausted, the local pool will not give out any more address, but GGSN doesn't cancel radius authentication request. The PDP is not created, but negative response is not sent back either.

  Work around: To avoid this problem, user can config a very big local pool, so that address will not be exhausted until we have a fix for it.

- CSCea61911

  A Cisco router running Gateway GPRS support node (GGSN) does not send a accounting-stop in case of authentication failure.

  An incoming create PDP context request from MS fails to authenticate on GGSN.

  There are no known workarounds.

- CSCea63657

  Issuing the **clear gprs gtp pdp context all** command while radius accounting requests are pending may cause GGSN to reload.

  There are no known workarounds.

- CSCea67414

  Cisco GGSN may show a large value (negative value) for counters “activated v0 pdp” and/or “activated v1 pdp”, under the **show gprs gtp status** command when GGSN receives a version 0 (v0) create request for an existing v1 Packet Data Protocol (PDP) context or vice-versa.

  This only occurs when the GGSN receives create pdp request of different GPRS Tunneling Protocol (GTP) version than the PDP was originally created with.

  There are no known workarounds.

- CSCea67422

  Cisco GGSN sometimes reloads when the SGSN falls back to gtpv0 and GGSN detects a path failure.

  There are no known workarounds.

- CSCea70814

  To prevent GGSN from completely running out of memory due to abnormal conditions, such as CG down, GGSN will stop processing Charging triggers when the memory runs dangerously low. The default threshold is 50MB. When this happens, GGSN will reject new PDP created requests with cause value “no resource” and the following charging triggers will be ignored:

  – Volume limit triggers that have occurred due to ongoing traffic on existing PDPs
  – QoS changes
  – Tariff changes
  – SGSN changes
  – Partial CDR closures issued from CLI

  Note, however, that the byte counts are still kept and will be reported after the GGSN recovers. Since some change conditions are not handled, some of the byte counts will not have the accurate charging condition, i.e. QoS and tariff. However there is no corruption in the CDRs and the CDRs conforms to all CDR encoding rules. It is just as if those triggers never happened.

  The Caveat here is that some CDRs will have incorrect charging condition due to the non-handling of tariff and QoS triggers.

  This situation occurs when GGSN is in relatively high load, in terms of ongoing traffic, and PDP create/delete/udpates. CGs are down and CDR’s can not be sent out.

  There are no known workarounds, but every measure should be taken to ensure that at least one CG is always up and connected to the GGSN via reliable network. Locally and directly connected CGs are highly recommended.

- CSCea80864

  When IP local pool is used for address allocation of Dynamic PDP contexts, Processor memory leak is noticed when the pool is exhausted and GGSN still tries to allocate address from this pool.

  There are no known workarounds. However, careful planning of the IP address pool may help to some extent.

- CSCea84750

  There is a processor memory leak in SNMP when APN’s are created and then deleted using SNMP object cgprsAccPtRowStatus in the CISCO-GPRS-ACC-PT-MIB.my

  This problem is observed on a 7200 Cisco router running 122-8YW1 image and with the GGSN service enabled.

  There are no known workarounds.

- CSCin24248

  When a Cisco router running Gateway GPRS Support node (GGSN) software receives a radius authentication failure after dhcp has returned an ip address but still in process, there is a possibility of router reload.

  There are no known workarounds.

- CSCin13431

  When Cisco Router runs with R3.0 GGSN Image c7200-g5js-mz and we set the access-point configs through snmp set, the word “vrf” is appended to apn name.

  There are no known workarounds.

- CSCin26358

  GGSN may crash under the following extreme conditions:

  – Both CG are down for a significant amount of time so that CDR's buffered reaches over 600000.

  – Path failure happens at this time.

  – System runs out of process and IO memory.

  There are no known workarounds.

- CSCin29601

  If Gn interface is brought down when there are large number of PDP active, the IO memory runs out and the following tracebacks appear in the Cisco R4.0 GGSN console:

```
-Process= "GTP PDP Cleanup Process", ipl= 0, pid= 120
-Traceback= 6075E81C 6075FBD0 60701F80 607022E4 607028C8 6003D778 6003D9FC
60038
E34 60042424 611D2290 60042454 6004270C 60753BCC 60753BB8
tb12-7200g#
%SYS-2-MALLOCFAIL: Memory allocation of 788 bytes failed from 0x60701F78,
alignm
ent 32
Pool: I/O  Free: 3136  Cause: Memory fragmentation
Alternate Pool: None  Free: 0  Cause: No Alternate pool
```

  Running out of IO memory is a dangerous situation. It can cause ping to fail and the box to become unmanageable and inaccessible, and the TCP connection used by Charging can not be established.

  This problem occurs when a large number (over 50K) of PDPs exist on the path. The path fails due to a restart counter or interface down.

  There are no known workarounds.

- CSCin30772

  A Cisco Router running Gateway GPRS Support node (GGSN) release 3.0 software may reload while executing **show gprs gtp pdp access-point <number>** command.

  This might happen when we are in the process of displaying the pdp entries and if somehow the current pdp entry gets deleted from some other path. Hence this is a race condition and happens only in some corner case situations and has no impact on the performance or the functionality of the product.

  There are no known workarounds.

- CSCin31879

  CISCO GGSN reloads while creating more than 150k ip static pdps when 8k ppp pdp sessions were existed.

  The reason for this is low memory situation caused by CDR accumulation.

  If charging is enabled but no charging gateway configured, then we continue to create and accumulate CDRs and deplete all the available processor memory. This will lead to the problem of GGSN getting reloaded.

  Workaround: Disable charging with the **gprs charging disable** command.

- CSCin34191

  If the customer configures UMTS QoS and the MIB runs into infinite loop, the customer will have to fall back to canonical and delay QoS.

  There are no known workarounds.

- CSCin34816

  On a Cisco Router running GGSN 3.1 image, memory leak is observed when the following tables or columnar objects of the table are retrieved:

  – cGgsnHistNotifTable,

  – cgprsCgAlarmHistTable,

  – cgprsAccPtExtTable.

  There are no known workarounds.

- CSCin35416

  This problem happens with the Cisco GGSN release 12.2(8)YW after the suppression of the PPP control and address fields is implemented. With or without such field suppression, the lengths of PPP packets are incorrectly set so that IPCP packets are not properly switched to the LNS from the GGSN/LAC. Thus, no L2TP sessions could be successfully established for these PPP PDP contexts.

  Workaround: Turn CEF off, though this will significantly reduce the activation rate and the throughput of the GGSN.

- CSCin35720

  This is a CLI problem. Before the fix, under APN, we can config ip-address-pool dhcp-proxy-client <poolname>, which invalid.

  Also when we remove “ip-address-pool local <poolname>” the “<poolname” may appear in the previous config line.

  There are no known workarounds.

- CSCin37030

  Cisco GGSN 4.0 shows symptoms of processor memory leak with local authentication and accounting disabled.

  With accounting disabled and local authentication configured, if GTP version 1 PDP contexts are created at high rate and deleted, after a few repititon of this sequence free processor memory in the router decreases.

  There are no known workarounds.

- CSCin37626

  Cisco Router running Gateway GPRS Support Node (GGSN) rel 3.0 may software reload while executing **show gprs gtp path all** command when large no of sgsn paths are there in the system.

  There are no known workarounds.

- CSCin38469

  For a duplicate address scenario, GGSN sends trap with varbind value as “apnUnreachable(10)” for cGgsnHistNotifType, rather it should be authenticationFail(9).

  There are no known workarounds.

- CSCin40563

  Cisco router running Gateway GPRS Service node software deletes all the pdp context for a particular SGSN when it receives a update request with no recovery i.e. The scenario under which it happens is are as follows:

  1) from SGSN1 create a pdp context for a MS x

  2) send update context request for MS x from SGSN2 with recovery i.e. present in it, the one for the second SGSN

  3) Again send update context request for MS x from SGSN1 with no recovery i.e. present in it.

  There are no known workarounds.

- CSCin41811

  CISCO GGSN Running R4.0 does not clear ppp l2tp (ppp session terminating on LNS) pdp on execution of clear gprs gtp pdp all.

  Workaround: Use clear vpdn tunnel.

  Alternative workaround: Send the delete request to GGSN.

  The **show gprs gtp ms all** command does not list ppp l2tp sessions because ggsn does not know the ms ip address.

  Workaround: The ppp l2tp session can be listed by other show commands such as **show gprs gtp pdp access-point**.

- CSCin42763

  Cisco GGSN running with R4.0 image not sending the recovery IE information in the create pdp context response message to the SGSN (when the SGSN contacted first time with this GGSN).

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(8)YW

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YW and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx01088

  GGSN does not send “ICMP Host Unreachable” message to PDN.

  This situation occurs when GGSN is configured to use CEF.

  There are no known workarounds.

- CSCdx45096

  Cisco router running GGSN 12.2(8)YD GGSN image does not send downstream T-PDU’s when creating PDP contexts for vrf under specific conditions.

  This situation occurs under the following conditions:

  – Configure ip cef and 2 vrf instances and ensure that vrf is functioning correctly.
  – Unconfigure ip cef by executing “no ip cef”.
  – Save the configuration and reload the router.
  – Reconfigure ip cef and the apn’s for vrf.
  – Create a PDP context for vpn1 and vpn2

  - Send traffic downstream for vpn1 pdp context from the PDN.
  - T-PDU is not sent to the SGSN by the GGSN even after cef adjacency is established DS traffic is not sent to the SGSN.

  There are no known workarounds.

- CSCdz25552

  After reload, the NAT does not work. The NAT translation has to be reconfigured in order to make it work.

  Workaround: Reconfigure the NAT translation command.

- CSCdz32592

  When a charging tariff expires, a container has to be added to the CDR for every PDP. A percentage of these CDR's will also, as a result, reach the change limit and get closed, be encoded and put on the outgoing queue on the Ga. If there are a large number of PDP's, this will create a few minutes of spike in which the CPU utilization reaches 100%. If at this time traffic is running near capacity, some increase in the dropped packets will occur. Signally packets will also get affected.

  This situation occurs under the following conditions:

  - Large number of PDP's exist.
  - Tariff time is configured.
  - Data and signally traffic is running at near capacity.

  There is no known workarounds.

- CSCin22263

  When A secondary PDP Context Create Request is received without the linked NSAPI IE, the statistics from show gprs gtp statistics for mandatory IE missing is not updated.

  There are no known workarounds.

- CSCin24118

  GGSN crashes under the following specific scenario:

  - - Create a pdp context with ip address assigned from radius.
  - - Remove the "aaa accounting network <groupname> start-stop group <groupname>"
  - - Configure it back.
  - - Delete the session using "clear gprs gtp pdp all"
  - - Now send the same Create pdp context req.

  There are no known workaround.

- CSCin26358

  GGSN may crash under the following extreme conditions:

  - Both CG are down for a significant amount of time so that CDR's buffered reaches over 600000.
  - Path failure happens at this time.
  - System runs out of process and IO memory.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(8)YW

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.2(8)YW.

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family. 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 53
- Platform-Specific Documents, page 54
- Feature Modules, page 54
- Cisco IOS Software Documentation Set, page 55

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **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 12.2*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 YW" in these release notes, see *Caveats for Cisco IOS Release 12.2* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

- *Caveats for Cisco IOS Release 12.2 T*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 YW" in these release notes, see *Caveats for Cisco IOS Release 12.2 T* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2 T.

  On Cisco.com at:

Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, 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/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

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

- *Cisco 7000 User Guide*
- *Cisco 7000 Hardware Installation and Maintenance*

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Core/High-End Routers**

  On the Documentation CD-ROM at:

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

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(8)YW3 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 Configuration: **Cisco IOS Release 12.2**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **New Feature Documentation**

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: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Cisco IOS Release 12.2 Documentation Set Contents

Table 8 lists the contents of the Cisco IOS Release 12.2 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.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 8 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *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
• *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
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *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
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 8 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	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
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 8 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through 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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 53.