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

July 16, 2004

Cisco IOS Release 12.2(8)YY4

OL-3744-05

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(8)YY4. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(8)YY4, see the "Important Notes" section on page 9 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://www.cisco.com/warp/public/732/docsurvey/rtg/ to give us your feedback .

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)YY4 and includes the following sections:

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YY4

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-g5jk8s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g5jk9s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g5js-mz	48 MB	256 MB	RAM

Table 2 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YY3

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-g5jk8s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g5jk9s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g5js-mz	48 MB	256 MB	RAM

Table 3 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YY2

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-g5jk8s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g5jk9s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g5js-mz	48 MB	256 MB	RAM

Table 4 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YY1

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-g5jk8s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g5jk9s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g5js-mz	48 MB	256 MB	RAM

Table 5 Images and Memory Recommendations for Cisco IOS Release 12.2(8)YY

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-g5jk8s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g5jk9s-mz	48 MB	256 MB	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g5js-mz	48 MB	256 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(8)YY4 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 YY Software (c7200-g5js-mz), Version 12.2(8)YY4, 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 YY supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2 YY 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 6 lists the features and feature sets supported by the Cisco 7000 family in Cisco IOS Release 12.2(8)YY4 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)YY means a feature was introduced in 12.2(8)YY. 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 6 Feature List by Feature Set for the Cisco 7200 Series

		Software Images by Feature Sets			
Features	In	Gateway GPRS Support Node (GGSN) DES	Gateway GPRS Support Node (GGSN) 3DES	Gateway GPRS Support Node (GGSN)	
GGSN 3.1	(8)YY	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 YY.

New Hardware Features in Cisco IOS Release 12.2(8)YY4

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY4.

New Software Features in Cisco IOS Release 12.2(8)YY4

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY4.

New Hardware Features in Cisco IOS Release 12.2(8)YY3

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY3.

New Software Features in Cisco IOS Release 12.2(8)YY3

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY3.

New Hardware Features in Cisco IOS Release 12.2(8)YY2

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY2.

New Software Features in Cisco IOS Release 12.2(8)YY2

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY2.

New Hardware Features in Cisco IOS Release 12.2(8)YY1

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY1.

New Software Features in Cisco IOS Release 12.2(8)YY1

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YY1.

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

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

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

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

GGSN 3.1

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.

Packet of Disconnect (POD) feature

Platforms: Cisco 7200 series routers

The Packet Of Disconnect (POD) feature on GGSN gives an external IP node the ability to terminate a user session by sending a POD packet. The POD packet is a Radius Disconnect Req message. The contents of this message is not yet standardized and is hence Cisco proprietary. The primary motivation of POD support on GGSN comes from the billing requirements (both Pre-Paid & Hot Billing) wherein a user session (PDP context) on GGSN can be terminated from an external entity. However, the scope of the POD feature is not limited to just the billing requirements.

Cisco's POD implementation uses Radius messages (Disconnect Request, Disconnect Ack/Nak) and attributes described in RFC 2882 and RFC 2865. The 'Disconnect Request' message in addition contains the attributes 3GPP-IMSI and 3GPP-NSAPI (3GPP attributes) and optional 'Teardown indicator' (Cisco attribute). The GGSN upon receiving the Disconnect Request message, uses IMSI and NSAPI to identify the PDP context for a user and terminates the PDP context. If 'Teardown indicator' is also included in the message, the GGSN terminates all PDP contexts for that user which share the same PDP address (applicable only for GTPv1). The GGSN then sends Disconnect Ack/Nak (no attributes) response.

In order to configure POD on GGSN, the following CLI is used:

aaa pod server [port <port number>] server-key <string>

The port defaults to the UDP port 1700 on GGSN. This is the port on which, GGSN listens for the POD request

Interim Accounting Support

Presently, the GGSN sends an Accounting-Request START message to the AAA server upon PDP context creation and Accounting-Request STOP message upon the PDP context deletion. The Interim Accounting feature will enable the GGSN to send Accounting-Request INTERIM-UPDATE (IAU) messages to the AAA server during the lifetime of a PDP context. The IAU message is sent only when an 'Update Context Request' or a new 'Create Context Request' is received for an existing PDP context from the SGSN indicating changes to certain parameters (SGSN Signaling address, QoS negotiated) only. This feature is a value-added feature to facilitate IP based billing.

This feature is first switched on at the box level and then enabled/disabled for each required APN. The box level CLI command is as follows:

aaa accounting update newinfo

The APN level enabling of the feature is done by selecting the appropriate APN and then entering the following CLI:

Router (config-access-point) **[no] aaa-accounting interim update**

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

AGENT-CAPABILITIES for the corresponding MIBs can also be obtained from the above location.

The GPRS specific capability files are

- CISCO-GTP-CAPABILITY.my
- CISCO-GGSN-CAPABILITY.my
- CISCO-GPRS-ACC-PT-CAPABILITY.my
- CISCO-GPRS-CHARGING-CAPABILITY.my
- CISCO-GGSN-QOS-CAPABILITY.my

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 7.

Table 7 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

Behavior Changes in Cisco IOS Release 12.2(8)YY3

To allow the configuration of the DNS/NBNS address at the APN level, the following two commands are introduced as part of ddts CSCea48277.

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

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

The ddts CSCea91875 add the support for non-default vpdn domain-delimiters, using the global configuration command **vpdn domain-delimiter**.

Caveats for Cisco IOS Release 12.2 YY

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)YY4.

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 8 Caveats Reference for Cisco IOS Release 12.2 YY

DDTS Number	Open in Release	Resolved in Release
CSCdu53656		12.2(8)YY3
CSCdw20770	12.2(8)YY1	
CSCdw28703	12.2(8)YY, 12.2(8)YY1	
CSCdw35157		12.2(8)YY4
CSCdw42791		12.2(8)YY4
CSCdw56516		12.2(8)YY4
CSCdw59078	12.2(8)YY, 12.2(8)YY1	
CSCdx16321		12.2(8)YY3
CSCdx18932	12.2(8)YY3, 12.2(8)YY4	
CSCdx32495		12.2(8)YY4
CSCdx36197		12.2(8)YY4
CSCdx46375		12.2(8)YY4
CSCdx56743		12.2(8)YY4
CSCdx63927		12.2(8)YY3
CSCdx77088		12.2(8)YY3
CSCdy07908		12.2(8)YY3
CSCdy25990		12.2(8)YY1
CSCdy34494		12.2(8)YY4
CSCdy41412		12.2(8)YY4
CSCdy45150		12.2(8)YY3
CSCdy53351		12.2(8)YY1
CSCdy65242		12.2(8)YY1
CSCdy65416		12.2(8)YY1
CSCdy70927		12.2(8)YY4
CSCdy74135		12.2(8)YY1
CSCdy76805		12.2(8)YY4
CSCdy87641		12.2(8)YY2
CSCdz15747		12.2(8)YY1

Table 8 Caveats Reference for Cisco IOS Release 12.2 YY (continued)

CSCdz17155		12.2(8)YY4
CSCdz20666		12.2(8)YY1
CSCdz29765	12.2(8)YY2, 12.2(8)YY3	
CSCdz29773	12.2(8)YY2, 12.2(8)YY3	12.2(8)YY4
CSCdz32367	12.2(8)YY2	12.2(8)YY3
CSCdz33537		12.2(8)YY1
CSCdz38258	12.2(8)YY, 12.2(8)YY1	
CSCdz39284		12.2(8)YY2
CSCdz41124		12.2(8)YY2
CSCdz52774		12.2(8)YY1
CSCdz55751		12.2(8)YY1
CSCdz71127		12.2(8)YY3, 12.2(8)YY2
CSCdz73994		12.2(8)YY3
CSCdz77088	12.2(8)YY, 12.2(8)YY1	12.2(8)YY3
CSCdz79921	12.2(8)YY2	
CSCdz83042		12.2(8)YY1
CSCea00332	12.2(8)YY2	
CSCea02355		12.2(8)YY3, 12.2(8)YY2
CSCea06252		12.2(8)YY2
CSCea15645	12.2(8)YY2	12.2(8)YY3
CSCea16969	12.2(8)YY1	
CSCea17365	12.2(8)YY2	
CSCea17967	12.2(8)YY2	
CSCea22854		12.2(8)YY2
CSCea26072	12.2(8)YY2, 12.2(8)YY3, 12.2(8)YY4	
CSCea28131		12.2(8)YY3
CSCea28346		12.2(8)YY3
CSCea29085		12.2(8)YY2
CSCea30807	12.2(8)YY3	12.2(8)YY4
CSCea31687		12.2(8)YY2
CSCea40773		12.2(8)YY2
CSCea42294		12.2(8)YY4
CSCea48277		12.2(8)YY3

Table 8 Caveats Reference for Cisco IOS Release 12.2 YY (continued)

CSCea61911	12.2(8)YY2	12.2(8)YY3
CSCea63657		12.2(8)YY3
CSCea70814		12.2(8)YY4
CSCea75343		12.2(8)YY4
CSCea80864		12.2(8)YY3
CSCea86462		12.2(8)YY3
CSCea89536		12.2(8)YY3
CSCea91875		12.2(8)YY3
CSCea93875		12.2(8)YY4
CSCeb02935		12.2(8)YY4
CSCeb09237		12.2(8)YY4
CSCeb10298		12.2(8)YY3
CSCeb10788		12.2(8)YY3
CSCeb14701		12.2(8)YY3
CSCeb18325		12.2(8)YY3
CSCeb22043	12.2(8)YY3	
CSCeb30794		12.2(8)YY3
CSCeb34080		12.2(8)YY3
CSCeb39251		12.2(8)YY3
CSCeb40561		12.2(8)YY4
CSCeb42554		12.2(8)YY4
CSCeb50871		12.2(8)YY4
CSCeb71522		12.2(8)YY4
CSCeb73365		12.2(8)YY4
CSCec12828	12.2(8)YY4	
CSCin08450		12.2(8)YY1
CSCin16079		12.2(8)YY1
CSCin22269		12.2(8)YY1
CSCin22343	12.2(8)YY2	12.2(8)YY3
CSCin22472	12.2(8)YY2	
CSCin23191		12.2(8)YY1
CSCin23948	12.2(8)YY2	
CSCin26142	12.2(8)YY2	
CSCin27701	12.2(8)YY2	
CSCin28880	12.2(8)YY2	
CSCin28922		12.2(8)YY4
CSCin30231	12.2(8)YY4	

Table 8 Caveats Reference for Cisco IOS Release 12.2 YY (continued)

CSCin30772		12.2(8)YY1
CSCin34816		12.2(8)YY2
CSCin35685	12.2(8)YY2	
CSCin37030		12.2(8)YY3
CSCin37626	12.2(8)YY2	12.2(8)YY3
CSCin38611	12.2(8)YY2, 12.2(8)YY3, 12.2(8)YY4	
CSCin38708	12.2(8)YY2	
CSCin39610		12.2(8)YY3
CSCin40107	12.2(8)YY2	
CSCin40563		12.2(8)YY3
CSCin43269	12.2(8)YY3	12.2(8)YY4
CSCin44822	12.2(8)YY4	
CSCin45222		12.2(8)YY4
CSCin46829	12.2(8)YY4	
CSCin46941		12.2(8)YY4
CSCin47452		12.2(8)YY3
CSCin48184	12.2(8)YY3	12.2(8)YY4
CSCin49271		12.2(8)YY4
CSCin49460		12.2(8)YY4
CSCin51543		12.2(8)YY4
CSCin53181		12.2(8)YY4
CSCuk34244		12.2(8)YY4

Open Caveats—Cisco IOS Release 12.2(8)YY4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YY4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx18932

  GGSN ip address, becomes 0 if the user configures ip unnumber on the GGSN virtual template.

  There are no known workarounds.

- CSCea26072

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

  Charging must be enabled on GGSN and a MS address is 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.

- CSCec12828

  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.

- CSCin30231

  CISCO GGSN is incrementing ppp_regen_pending_peak counter of shGprsGtpStatistics abnormally, in case ppp-regen sessions are cleared by clearVpdnTuL2tpAll after reaching the configured max-pending value by using the hidden command **gprs gtp ppp-regeneration max-pending**.

  There are no known workarounds.

- CSCin38611

  When 300 VRF instances are created and deleted on a Cisco router running GPRS Gateway Support node software (GGSN) release 3.1, a memory leak is observed. This is a corner case and requires around 300 VRF instances to be created and then deleted on the GGSN to observe the problem.

  There are no known workarounds.

- CSCin44822

  Stale ppp-regen sessions will be left in CISCO GGSN when multiple sessions were deleted using "clear gprs gtp pdp all" while there was uplink/downlink traffic through all/some of the sessions.These stale sessions can be cleared using CLI "clear vpdn tunnel l2tp all"

  Workaround: Delete the sessions using "clear vpdn tunnel l2tp all".

- CSCin46829

  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.

Resolved Caveats—Cisco IOS Release 12.2(8)YY4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YY4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw35157

  Defining the AAA Server group on the c10k display the following message after a C10k power cycle:

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

  The functionality is not affected by the message.

  There are no known workarounds.

- CSCdw42791

  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.

  Alternative workaround: If RADIUS authentication is used, omit the "class" attribute from the RADIUS user profile.

- CSCdw56516

  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.

- CSCdx32495

  A Cisco router configured with crypto might reload.

  There are no known workarounds.

- CSCdx36197

  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.

  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
  ```

  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.

- CSCdx46375

  as5400 might experience 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

  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.

- CSCdy34494

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

  There are no known workarounds.

- CSCdy41412

  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 problem 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 problem may also occur in Release 12.2 T.

  There are no known workarounds.

- CSCdy70927

  Cisco router running Gateway GPRS Support (GGSN) IOS software may leak message buffer

  This happens when Cisco 7200 GGSN running 12.2(8)YY image switches primary and secondary charging gateways, the Echo Request message buffer will be leaked.

  There are no known workarounds.

- CSCdy76805

  On a Cisco router, if a list of AAA servers are configured, and if the one of these AAA servers is mis-configured without a secret and if there is no global radius secret configured, AAA fails to try the rest of the configured servers.

  If a AAA request is being retried across multiple radius servers due to no responses, and if one of these radius server is configured without a secret, AAA does not further retry to rest of the servers in the list.

  Workaround: Configure a proper radius secret for all radius servers or configure a global radius secret.

- CSCdz17155

  First two servers change there state from “DEAD” to “UP” within deadtime.

  The problem happens when several RADIUS servers is configured.

  There are no known workarounds.

- CSCdz29773

  Cisco router running GGSN Release 3.1 image (12.2(8)YY3) may be left with some stale PDP contexts (contexts which cannot be deleted) when initiating PDP deletion in low memory condition.

  This may happen only if charging is enabled on GGSN and the GGSN is running low on memory and we initiate deletion of the PDP contexts at that time so that the GGSN is not able to get enough buffer to close the CDR.

  There are no known workarounds.

- CSCea30807

  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

  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.

- CSCea70814

  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 reject 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.

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

  When this does happen, there is currently no workaround, 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.

- CSCea75343

  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:

  - Configure the global AAA server
  - Configure the AAA server group

- CSCea93875

  When memory threshold (gprs memory threshold <100KBytes>) is reached, the PDP that is experiencing certain updates, e.g. SGSN change or QoS is supposed to cause the PDP to be deleted to regain memory. But the PDP is still there. It is only deleted after a volume limit is reached.

  This occurs under the following conditions:

  - gprs memory threshold is configured.
  - GGSN memory runs below the threshold.

  Workaround: Delete the PDP by CLI or sending traffic.

- CSCeb02935

  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 configuration related to CDR transfer should reduce the chance of this leak.

- CSCeb09237

  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.

- CSCeb40561

  On Cisco IOS 12.2(8) YW & YY releases, 12.2T, 12.3, 12.3T, the router may crash if it is low on processor memory and SNMP get operations are done on OSPF MIBs.

  There are no known workarounds.

- CSCeb42554

  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.

- CSCeb50871

  Cisco 7200 series router running Release 3.1 Gateway GPRS Support Node (GGSN) IOS software shows incorrect value of the field “number of ip_address_allocated” in the output of the command **show gprs access-point <apn-index>**.

  The counter “number of ip_address_allocated” in the output of the command **show gprs access-point <apn_index>** is incorrectly decremented by 2 instead of by 1 upon every pdp context deletion. This only seems to happen when using RADIUS as an IP address allocation mechanism. Also, the “number of ip_address_allocated” is incorrectly decremented by 1 after rejecting a pdp create context request (with a different TID) for an already existing pdp context. This second issue seems to happen for IP address allocation through DHCP as well as through RADIUS.

  These issues are also seen when retrieving the MIB objects: cgprsGtpNumAllocIpAddr and cgprsGtpTotalNumAllocIpAddr via SNMP.

  There are no known workarounds.

- CSCeb71522

  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.

- CSCeb73365

  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.

  Alternative workaround: Configure memory protection on the GGSN.

- CSCin28922

  SSG does not send any connection accounting records.

  This problem was found on Cisco IOS 7200 platform. But it is common to all platforms supporting SSG

  There are no known workarounds.

- CSCin43269

  Cisco router running Gateway GPRS Service node software reloads when we have a SGSN address same as CG address Image: c7200-g5jk8s-mz

  Workaround: Have a different IP address for CG and SGSN

- CSCin45222

  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.

- CSCin46941

  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

  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: Use the default vpdn domain-delimiter which is “@”.

- CSCin49271

  On a Cisco router running Gateway GPRS support node (GGSN) image 12.2(8)YY3, may run into a situation where PDP context deletion initiated from GGSN side (for e.g. by using “clear gprs gtp pdp all”) does not succeed anymore. Some tracebacks may also be encountered.

  This scenario is triggered by a rare race condition related to create PDP context request message received for an existing PDP context that is in awaiting delete PDP response message from SGSN.

  There are no known workarounds.

- CSCin49460

  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.

- CSCin51543

  Tracebacks are seen in CISCO GGSN while creating ppp-regen pdp under the following two conditions

  - verify-domain feature is configured
  - vpdn domain-delimiter is other than the default '@'

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

- CSCin53181

  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.

- CSCuk34244

  This problem may be seen on Cisco 7200 or Cisco 7400 platforms when a packet is received via one tunnel and CEF-switched into another tunnel. If a condition occurs after the first tunnel encapsulation has been replaced with the second tunnel encapsulation that requires the newly tunnel-encapsulated packet to be punted from CEF switching to a slower switching path, the router may reload with a DMA error.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(8)YY3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YY3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx18932

  GGSN ip address, become 0 if the user configures ip unnumber on GPRS virtual template.

  There are no known workarounds.

- CSCdz29765

  CISCO GGSN YY Release may have stale PDPs when:

  1. GGSN receives duplicate creates for the PDPs in the process of deletion,

  2. GGSN PDP deletion is simultaneously invoked by multiple causes, for example, GGSN initiates PPP PDP deletion due to IPCP failure, while user execute CLI command clear gprs gtp pdp all

  3. GGSN is in low memory condition when initiating PDP deletes

  There are no known workarounds.

- CSCdz29773

  CISCO GGSN Release YY may have stale PDPs when initiating PDP deletion in low memory condition.

  There are no known workarounds.

- CSCea26072

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

  Charging must be enabled on GGSN and a MS address is 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.

- CSCea30807

  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.

- CSCeb22043

  The NAS IP address attribute contains wrong value in radius authentication and accounting requests, if VRF aware radius server is used.

  The NAS IP address attribute in radius request should contain, by default, the IP address of the outgoing interface. If VRF aware radius server is used (“server-private” and “ip vrf forwarding” under aaa group config), this attribute contains a address of some other interface on GGSN.

  There are no known workarounds.

- CSCin38611

  When 300 VRF instances are created and deleted on a Cisco router running GPRS Gateway Support node software (GGSN) release 3.1, a memory leak is observed. This is a corner case and requires around 300 VRF instances to be created and then deleted on the GGSN to observe the problem.

  There are no known workarounds.

- CSCin43269

  Cisco router running Gateway GPRS Service node software reloads when we have a SGSN address same as CG address Image: c7200-g5jk8s-mz

  Workaround: Have different IP address for CG and SGSN

- CSCin48184

  CISCO GGSN ppp-regen verify-domain feature does not work in case vpdn domain-delimiter is other than the default "@"

  Workaround: Use the default vpdn domain-delimiter which is "@".

Resolved Caveats—Cisco IOS Release 12.2(8)YY3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YY3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdu53656

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- CSCdx16321

  On a 7206VXR router running 12.1(11b)E with GRE/IPSEC tunnels and certain SNMP traps enabled, spurious memory accesses and alignment errors are recorded:

  ```
  *Mar 24 21:24:09 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, c
  hanged state to up
  *Mar 24 21:24:58 UTC: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x613BBA
  F8 reading 0x0
  *Mar 24 21:24:58 UTC: %ALIGN-3-TRACE: -Traceback= 613BBAF8 613042E8 613026B8 612
  FF464 60AC5E5C 60AC6228 60ADA34C 6130E048
  *Mar 24 21:24:58 UTC: %ALIGN-3-TRACE: -Traceback= 613BBAFC 613042E8 613026B8 612
  FF464 60AC5E5C 60AC6228 60ADA34C 6130E048
  ```

  This appears to be due to having certain SNMP traps enabled:

  ```
  snmp-server enable traps ipsec tunnel start
  snmp-server enable traps ipsec tunnel stop
  ```

  Workaround:

  ```
  no snmp-server enable traps ipsec tunnel start
  no snmp-server enable traps ipsec tunnel stop
  ```

- 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.

  The 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.

- CSCdx77088

  Cisco router running GGSN image may see software forced reload due to “watchdog timeout in pool process” when running in low memory condition.

  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 problem is observed on a Cisco router.

  There are no known workarounds.

- CSCdy45150

  When the router receives a RADIUS response for which it has no matching request, it produces an AAA-3-SERVER_INTERNAL_ERROR and a traceback. This can happen when the radius server takes longer to respond than the configured timeout.

  In addition, the statistics reported by the AAA server MIB and “show aaa servers” about the number of unexpected responses are not properly incremented.

  If the problem is due to a slow radius server, you can decrease the frequency with which you get the error message by increasing the timeout.

  There are no known workarounds.

- CSCdz32367

  CISCO GGSN YY Release might leak memory in the following two cases:

  1. When receiving an incorrectly formatted charging response message

  2. When sending CDR records when charging path failed

  There are no known workarounds.

- CSCdz71127

  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

  Cisco GGSN sends bad authenticator in Radius messages under the condition wherein the Radius key configured is of a certain length. For example when the Radius key is of 8, 20 or 24 bytes long.

  Workaround: Configure the Radius Key having odd numbered length.

- CSCdz77088

  The value of field "primary nbns" is 0.0.0.0 in the output of **show gprs gtp pdp tid** command and the create response.

  This problem is observed in a Cisco 7200 router acting as GGSN, IP address allocated by Radius server and the user profile on the Radius server consists of following attributes:

  - Idle-Timeout
  - MS-Primary-DNS-Server
  - MS-Secondary-DNS-Server
  - MS-Primary-NBNS-Server
  - MS-Secondary-NBNS-Server

  Workaround: Configure the Idle Timeout value under the Access Point rather than in the user profile.

  Alternative workaround: Do not use Idle Timeout Attribute/MS-Primary-NBNS-Server in cases where not needed.

- 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

- 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.

- CSCea28131

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

  Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml.

- 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. So far, this limit is only hard-coded and not configurable.

  There are no known workarounds.

- CSCea48277

  To allow the configuration of the DNS/NBNS address at the APN level, the following two commands are introduced.

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

  There are no known workarounds.

- 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.

  The IOS **aaa accounting send stop-record authentication failure** command is used to send stop record on authentication failure. But this does not have any impact in the above case.

  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.

- 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. Careful planning of the IP address pool may help to some extent.

- CSCea86462

  In 12.2(8)YY2, CSCea31687 introduced a new hidden CLI to optionally use APN IE domain name for PPP-Regen. With this ddts, we make the CLI visible.

  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 requests with different sequence numbers.

  There are no known workarounds.

- CSCea91875

  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 **vpdn domain-delimiter** command.

  There are no known workarounds.

- CSCeb10298

  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

  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.

- CSCeb14701

  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.

- CSCeb18325

  After user add and VRF APN config, GGSN address is lost from global cef table.

  There are some sequence problem in creating vaccess for VRF.

  Workaround: Every time after changing GGSN config, do a **no ip cef** and **ip cef** again to reset CEF tables.

- CSCeb30794

  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.

- CSCeb34080

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

  There are no known workarounds.

- CSCeb39251

  This problem is found to have happened to Cisco GGSN Release 3.1 in 12.2(8)YY2, but is likely to be generic in releases R3.0 and R4.0 as well.

  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.

- CSCin22343

  On a cisco router running GPRS gateway support node (GGSN) image, GGSN may reload in case of high PPP-PDP creates, when we are getting ip address from dhcp at rate more than 10pps.

  When we send around 8k ppp pdp terminating at ggsn (with dhcp) with the rate of more than 10pps. After creating more than 5k sessions, all the sessions will go down due to high cpu utilization up to 100%. During this process or doing a clear gprs gtp pdp all at this stage may reload the GGSN.

  Workaround: Reduce the rate and get the ip address from the radius.

- CSCin37030

  Cisco GGSN 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 iteration of this sequence, free processor memory in the router decreases.

  There are no known workarounds.

- CSCin37626

  Cisco Router running Gateway GPRS Support Node (GGSN) may issue software reload in the following 2 cases

  1. while executing **show gprs gtp path all** command when large no of sgsn paths are there in the system.

  2. Similarly when **show gprs gtp pdp version** <> command is executed while large no of pdps are being deleted.

  There are no known workarounds.

- CSCin39610

  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.

- 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 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.

- CSCin47452

  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 **gprs charging disable** command before GGSN is put into operation.

Open Caveats—Cisco IOS Release 12.2(8)YY2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YY2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz29765

  CISCO GGSN YY Release may have stale PDPs when:

  - GGSN receives duplicate creates for the PDPs in the process of deletion
  - GGSN PDP deletion is simultaneously invoked by multiple causes, for example, GGSN initiates PPP PDP deletion due to IPCP failure, while user execute CLI command clear gprs gtp pdp all
  - GGSN is in low memory condition when initiating PDP deletes

  There are no known workarounds.

- CSCdz29773

  CISCO GGSN Release YY may have stale PDPs when initiating PDP deletion in low memory condition.

  There are no known workarounds.

- CSCdz32367

  CISCO GGSN YY Release might leak memory in the following two cases:

  1. when receiving an incorrectly formatted charging response message

  2. when sending CDR records when charging path failed

  There are no known workarounds.

- CSCdz79921

  When Cisco router running Gateway GPRS Service node software, is reloaded, the virtual access for the GTP shows as down incase the vtemplate for GTP is configured to take ip address from the loopback:

  ```
  Software: c7200-g5js-mz
  ```

  Workaround: When the router boots up under the virtual template configure “no encapsulation gtp”, configure “encapsulation gtp”.

- CSCea00332

  Cisco GGSN sends a response to the create request as “no resource” available instead of “service not supported” under the condition of duplicate IP Address being assigned to the PDP.

  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.

- 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.

- CSCea17967

  When “aggregate auto” is configured under an APN which uses local DHCP pool for dynamic address allocation, a default route via GTP vaccess is added to the route table similar to one shown below:

  ```
  U*   0.0.0.0/0 [1/0] via 0.0.0.0, Virtual-Access1
  ```

  This may cause network problems by directing a packet to GTP for which no matching route was found.

  Workaround: Don’t configure “aggregate auto” under an APN with local DHCP pool configuration. Configure an aggregate range instead.

- CSCea26072

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

  Charging must be enabled on GGSN and a MS address is 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.

- 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.

  The IOS **aaa accounting send stop-record authentication failure** command is used to send stop record on authentication failure. But this does not have any impact in the above case.

  There are no known workarounds.

- CSCin22343

  On a cisco router running GPRS gateway support node (GGSN) image, GGSN may reload in case of high PPP-PDP creates, when we are getting ip address from dhcp at rate more than 10pps.

  When we send around 8k ppp pdp terminating at ggsn (with dhcp) with the rate of more than 10pps. After creating more than 5k sessions, all the sessions will go down due to high cpu utilization up to 100%. During this process or doing a clear gprs gtp pdp all at this stage may reload the GGSN.

  Workaround: Reduce the rate and get the ip address from the radius.

- CSCin22472

  CISCO GGSN is not able to create thousands of successful PPP PDP sessions (terminating at GGSN) at a rate of more than 5pps and ip addresses are from DHCP

  This problem is not seen if rate is less than 5pps or if ip addresses are from RADIUS

  Workaround: Send the requests at a rate of less than 5pps or get the ip addresses from Radius.

- CSCin23948

  Cisco GGSN may reload when configured with a DFP agent.

  This crash happens when the following is configured:

  ```
  ip dfp agent gprs
      port <port #>
      inservice
  ```

  There are no known workarounds.

- CSCin26142

  When Gn/Ga goes down momentarily and comes back up (before GTP retry expires), GGSN sends Echo Request out more frequently than what has been configured.

  There are no known workarounds.

- CSCin27701

  When GGSN receives a Create PDP Context Request with the header length less than the total GTP packet length, the GTP message too short counter is not incremented.

  There are no known workarounds.

- CSCin28880

  A Cisco Router running Gateway GPRS Support node (GGSN) release 3.0 software throws up the following error while booting:

  ```
  %PARSER-4-BADCFG: Unexpected end of configuration file, if at all an access-point is
  configured under an access-point list.
  ```

  This is cosmetic bug and has no impact on the performance or the functionality of the product.

  There are no known workarounds.

- CSCin35685

  Currently the PDP context byte and packet counters in GGSN can support a maximum value of 4294967296. Counters overflow may happen if a context is up for a long time and is carrying a lot of traffic causing the values exceed this maximum limit and causing the counters roll over.

  There are no known workarounds.

- CSCin37626

  Cisco Router running Gateway GPRS Support Node (GGSN) release 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.

- CSCin38611

  When 300 VRF instances are created and deleted on a Cisco router running GPRS Gateway Support node software (GGSN) release 3.1, a memory leak is observed. This is a corner case and requires around 300 VRF instances to be created and then deleted on the GGSN to observe the problem.

  There are no known workarounds.

- CSCin38708

  On CISCO GGSN running 12.2(8)YY2 image, when GPRS service is configured on the router and if we try to deactivate the GDM service, the GPRS service will be deactivated and vice-versa.

  There are no known workarounds.

- CSCin40107

  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 eg: 1 min. Since reconnect echoes 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.

Resolved Caveats—Cisco IOS Release 12.2(8)YY2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YY2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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.

- 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.

- 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.

- CSCdz71127

  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

- 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

- 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.

  GGSN is in relatively high load, in terms of ongoing traffic, and PDP create/delete/updates.

  The prevention measure put in by this fix protects GGSN from completely run out of memory in such cases.

  A new CLI:

  ```
      "[no] gprs memory threshold <x>"
  ```

  where <x> is in 100KB, has been added to set a low memory watermark to prevent memory overload.

  The default value of memory threshold has been set to 1 (i.e.; 100 KB, as it is in 100KB units).

  When the amount of memory remaining on the box reaches the threshold, GGSN will:

  - reject new PDP create requests with cause value “no resource”
  - 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 GGSN will be in a stable mode, until the CGs are brought back online, at which time, buffered CDRs will be sent out and memory will be regained.

  Memory can also be regained as existing PDPs naturally die down or cleared from CLI.

  CDRs can also be clear from the CLI with the following commands:

  ```
  clear gprs charging cdr all|access-point|tid
  ```

which will cause CDRs to be closed without opening subsequent partial CDRs. In this case, the PDP's will be sustained except charging is not performed on them. This is an existing facility and can be used as a emergency measure.

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.

- CSCea22854

  The new command gprs watermark memory has some problems:

  When "no gprs watermark memory" or the default value of 512 is set, the running config would be saved wrongly (with a value of 0). And next time when the GGSN is reloaded, it will have parser errors due to the fact that "0" is in the valid range.

  Also the "no gprs watermark memory" does not work.

  After running config is saved when the "gprs watermark memory 512".

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

- 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 after unable to reach the CG, will give up trying.

  GGSN should try to reconnect by periodically detecting if the CG is up. If the link is down, and we can not send the echo, GGSN should enter a failed state which may or may not be able to recover without manual intervention/trouble shooting.

  This feature will only turned on when the hidden CLI "gprs charging reconnect <minutes>" is configured.

  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.

  GGSN selects a L2TP tunnel, either using an APN name or the user-supplied domain name. PPP-Regeneration on GGSN would always prioritize the user-supplied domain-name, over the APN name. Hence, irrespective of the APN the user is connecting to, GGSN would connect the user to the requested domain-name, using the L2TP tunnel for that domain.

  A new hidden command will be introduced under the APN sub-config: "ppp-regeneration verify-domain". If this command is applied to an APN, GGSN would check the domain sent in PCO options with the APN name. In case of mis-match, and if this command has been applied to the APN, the create request would be rejected with the cause value "Service not supported".

  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.

- CSCin34816

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

  - cGgsnHistNotifTable,
  - cgprsCgAlarmHistTable,
  - cgprsAccPtExtTable.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(8)YY1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YY1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw20770

  Cisco GGSN sets the cause value of the charging record closure to “0” which means normal closure, under the condition where in the relevant PDP is cleared/closed from the CLI. This should be set to “20” which is Management Intervention.

  There are no known workarounds.

- CSCdw28703

  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 symptom is observed on a Cisco 7500 series router.

  Workaround: Disable CEF.

- CSCdw59078

  PPPoE vacess interface will be created by default even the router does not config PPPoE. but it doesn’t have any impact on the function of the router.

  There are no known workarounds.

- CSCdz38258

  If a duplicate pdp context create request or update is sent to an existing PDP with different QoS delay class, the QoS delay class counters are not correct in “show gprs gtp status” command.

  There are no known workarounds.

- CSCdz77088

  The value of field “primary nbns” is 0.0.0.0 in the output of **show gprs gtp pdp tid** command and the create response.

  This symptom is observed in a Cisco 7200 router acting as GGSN, IP address allocated by Radius server and the user profile on the Radius server consists of following attributes:

  - Idle-Timeout
  - MS-Primary-DNS-Server
  - MS-Secondary-DNS-Server
  - MS-Primary-NBNS-Server
  - MS-Secondary-NBNS-Server

  Workaround: Configure the Idle Timeout value under the Access Point rather than in the user profile.

  Alternative workaround: Do not use Idle Timeout Attribute/MS-Primary-NBNS-Server in cases where not needed.

- CSCea16969

  CISCO router running with GGSN R3.0 and above image allows a PDP context with IP address same as CG IP address.

  There are no known workarounds

Resolved Caveats—Cisco IOS Release 12.2(8)YY1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YY1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdy25990

  CPU utilization is very high when traffic sent for non-existing PDP context.

  There are no known workarounds.

- CSCdy53351

  Cisco GGSN will leak memory if a new Create/Delete PDP request message is received on an existing PDP context that is awaiting Radius/DHCP server response.

  This occurs only if the Create/Delete PDP 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 the Radius or DHCP server for this context.

  There are no known workarounds.

- CSCdy65242

  When create access-point using VRF LOCAL DHCP server to allocate address, the VRF local DHCP server didn't response the DHCP discover msg. So address allocation will fail.

  Workaround: Users can either use 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 didn't response the DHCP discover msg. So address allocation will fail.

  Workaround: Users can either use global local DHCP server shared by multiple VRFs.

- CSCdy74135

  CDR is not sent immediately if CG comes back alive.

  This problem can be reproduce using the following steps:

  1. Establish a PDP context

  2. Deactive the primary CG and clear the CDR on GGSN and wait till Primary CG in params inactive.

  3. Now active primary CG and send node alive request.

  4. GPRS params got updated properly on the GGSN. But the CDR is sent only after 30 seconds.

  There are no known workarounds.

- CSCdz15747

  On a Cisco router running Gateway GPRS Support node software, the "charging container volume-threshold" limit configuration does not work as expected. The configuration is accepted and shown but the actual threshold is still set to the default value. This causes the containers to remain open even upon hitting volume limit.

  There are no known workarounds.

- CSCdz20666

  The configuration "gprs gtp map signalling tos" gets automatically when user enters "maximum-pdp-context-allowed". The behavior is observed when user loads CISCO router with the GGSN R3.0 image.

  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 workarounds.

- CSCdz52774

  Cisco 7200 Router running GGSN 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.

  It happens under the following specific race condition:

  After radius authentication and authorization are successful, but before sending back create response, process gets suspended and by chance 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.

- 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.

- CSCin08450

  The maximum number of supported PPP PDP context is 8000. The router may crash when creating more than 8000 contexts.

  There are no known workarounds.

- CSCin16079

  The problem is seen only when no-partial-cdr-generation is enabled.

  This problem can be reproduce using the following steps:

  1. Configure sgsn-change-limit as 0 and enable cdr-option no-partial-cdr-generation

  2. Create a PDP context and send traffic through it so that volume threshold is crossed and a partial CDR is opened.

  3. Now send an RA update request. Note that the partial CDR has not got closed now.

  There are no known workarounds.

- CSCin22269

  A Cisco router running Gateway GPRS support node (GGSN) software, does not allow MNC value zero to be configured.

  This affects users who need to configure MNC zero with the command “gprs mcc mnc”.

  There are no workarounds.

- CSCin23191

  When TCP is used as the charging path protocol, unacknowledged queued CD's were not sent out by the GGSN when the backup CG comes up in the following steps: scenario.

  The problem occur when the following steps are taken:

  1. Configure tcp as the path protocol and two CG's on the GGSN. (have cdr-aggregation-limit 1)

  2. Bring down or deactivate the Backup CG. GGSN has the TCP connection to the primary CG.

  3. Create a PDP context. Now, deactivate the primary CG. The TCP connection to this CG is cleared at the GGSN and the server switchover timer is started.

  4. Delete the PDP context now. After server switcover timer expires, the ggsn attempts to connect to the secondary CG but fails as the CG is deactivated and the cdr is queued.

  5. Now activate the backup CG and send a node alive message from it. GGSN reconnects to the backup CG and makes it the current active CG. However, the unacknowledged queued CDR's are not sent out to it.

  Note In scenarios where the GGSN has already connected to the backup cg and then the backup cg goes down and then comes back up, the queued CDR's are sent out to it properly.

  Workaround: Do a round of switch-over by bringing the primary down, then up, and then bring down the backup and then up.

- CSCin30772

  A Cisco Router running Gateway GPRS Support node (GGSN) release 3.0 software may reload while executing the **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.

Open Caveats—Cisco IOS Release 12.2(8)YY

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

- CSCdw28703

  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 symptom is observed on a Cisco 7500 series router.

  Workaround: Disable CEF.

- CSCdw59078

  PPPoE vacess interface will be created by default even when the router does not config PPPoE. However, this does not have any impact on the function of the router.

  There are no known workarounds.

- CSCdz38258

  If a duplicate pdp context create request or update is sent to an existing PDP with different QoS delay class, the QoS delay class counters are not correct in "show gprs gtp status" command.

  There are no known workarounds.

- CSCdz77088

  The value of field "primary nbns" is 0.0.0.0 in the output of "show gprs gtp pdp tid" command and the create response.

  This symptom is observed in a Cisco 7200 router acting as GGSN, IP address allocated by Radius server and the user profile on the Radius server consists of following attributes:

  - Idle-Timeout
  - MS-Primary-DNS-Server
  - MS-Secondary-DNS-Server
  - MS-Primary-NBNS-Server
  - MS-Secondary-NBNS-Server

  Workaround: Configure the Idle Timeout value under the Access Point rather than in the user profile.

  Alternative workaround: Do not use Idle Timeout Attribute/MS-Primary-NBNS-Server in cases where it is not needed.

Resolved Caveats—Cisco IOS Release 12.2(8)YY

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YY. 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)YY.

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 41
- Platform-Specific Documents, page 42
- Feature Modules, page 42
- Cisco IOS Software Documentation Set, page 42

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 "Important Notes" 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 "Important Notes" 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)YY2 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 9 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 9 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

Table 9 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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
• *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

Table 9 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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
• *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 40.