



# Release Notes for Cisco Cisco 7000 Family for Cisco IOS Release 12.2 YD

---

**January 27, 2003**

Cisco IOS Release 12.2(8)YD3

OL-2709-04

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(8)YD3. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(8)YD3, see the [“Caveats for Cisco IOS Release 12.2” section on page 13](#) and *Caveats for Cisco IOS Release 12.2*. 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.

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at <http://www.cisco.com/warp/customer/770/index.shtml>. If you do not have a Cisco.com login account, you can find field notices at <http://www.cisco.com/warp/public/770/index.shtml>.

## Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 4](#)
- [MIBs, page 6](#)
- [Important Notes, page 7](#)
- [Caveats for Cisco IOS Release 12.2, page 13](#)
- [Related Documentation, page 16](#)



---

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

Copyright © 2002-2003. Cisco Systems, Inc. All rights reserved.

- [Obtaining Documentation, page 22](#)
- [Obtaining Technical Assistance, page 23](#)

## System Requirements

This section describes the system requirements for Cisco IOS Release 12.2 YD and includes the following sections:

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

## Memory Recommendations

**Table 1** Images and Memory Recommendations for Cisco IOS Release 12.2 YD

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	Gateway GPRS Support Node Standard Feature Set	Gateway GPRS Support Node (GGSN) DES	c7200-g5jk8s-mz	48 MB	256 MB DRAM	RAM
		Gateway GPRS Support Node (GGSN) 3DES	c7200-g5jk9s-mz	48 MB	256 MB DRAM	RAM
		Gateway GPRS Support Node (GGSN)	c7200-g5js-mz	48 MB	256 MB DRAM	RAM

## Supported Hardware

Cisco IOS Release 12.2(8)YD3 supports the following Cisco 7000 family platforms:

- Cisco 7200 series routers

For detailed descriptions of the new hardware features, see the [“New and Changed Information” section on page 4](#).

For additional information about supported hardware for this platform and release, please refer to the Hardware/Software Compatibility Matrix in the Cisco Software Advisor at the following location:

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

## Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7200 software image with Cisco IOS Release 12.2(8)YD3:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 YD Software (c7200-g5js-mz), Version 12.2(8)YD3, RELEASE SOFTWARE
```

## Upgrading to a New Software Release

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

[http://www.cisco.com/warp/public/130/upgrade\\_index.shtml](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(8)YD3 supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(8)YD3 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](mailto:export@cisco.com).

---

[Table 2](#) lists the features and feature sets supported by the Cisco 7200 series routers in Cisco IOS Release 12.2(8)YD3 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)YD means a feature was introduced in 12.2(8)YD.

**Table 2** Feature List by Feature Set for the Cisco 7200 Series (continued)

Features	In	Software Images by Feature Sets		
		Gateway GPRS Support Node (GGSN) DES	Gateway GPRS Support Node (GGSN) 3DES	Gateway GPRS Support Node (GGSN)
GGSN 3.0	(8)YD	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 YD.

### New Hardware Features in Cisco IOS Release 12.2(8)YD3

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YD3.

### New Software Features in Cisco IOS Release 12.2(8)YD3

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YD3.

### New Hardware Features in Cisco IOS Release 12.2(8)YD2

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YD2.

### New Software Features in Cisco IOS Release 12.2(8)YD2

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YD2.

### New Hardware Features in Cisco IOS Release 12.2(8)YD1

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YD1.

## New Software Features in Cisco IOS Release 12.2(8)YD1

There are no new software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(8)YD1.

## New Hardware Features in Cisco IOS Release 12.2(8)YD

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

## New Software Features in Cisco IOS Release 12.2(8)YD

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

### GGSN 3.0

Platforms: Cisco 7200 series routers

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

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

GPRS introduces the following two new major network elements:

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

# MIBs

## Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

## Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-\* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in [Table 3](#).

**Table 3** *Deprecated and Replacement MIBs*

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

# Important Notes

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

## Migration to Virtual Route Forwarding (VRF) for GGSN R3.0

This section describes the engineering analysis of migrating CLI command **use-interface** to **vrf** command.

The **use-interface** command is designed to support private addressing when there was no general VPN support in IOS few years back. The implementation of the **use-interface** command is to by-pass routing and send VPN traffic directly to the interface associated with an APN when the **use-interface** command is configured for an APN. This approach is restrictive since there is a single global routing table, and the routing table is bypassed when the use-interface is used.

With GGSN R3.0, we provide a generic way of interfacing to any Virtual Private Network using the IOS element called VRF-Lite. VRF-Lite instance allows the operator to define multiple virtual contexts (VRF) inside the router. Each VRF consists of an IP routing table, a routing process, a forwarding engine, a set of interfaces, and a set of rules and routing protocol parameters that control the information that is included into the routing table. In addition to these, a separate DHCP or Radius server can be supported in the VRF domain. These separate tables and process prevent information from being forwarded outside a VPN, and also prevent packets that are outside a VPN from being forwarded to a router within the VPN. Since we can add or subtract interface to or from the VRF easily, we can create a VRF with as many interfaces as we want. It is very flexible and scalable. We can apply policies to each VRF separately and not affecting others. Since it is provided by IOS core, there are many related features on the road map so GPRS can benefit from all the new features.

We are aware of the changes will impact current users so we put in some effort to evaluate if the two commands can co-exist initially and the **use-interface** command can be phased out gradually. The engineering analysis is the co-exist of the two cannot be achieved without significant effort due to we'll need to maintain the new and old way to lookup a PDP context and do not get confused. Also the longer we wait to make the change, the more customers will be impacted.

For these reasons, we shall migrate the **use-interface** command to VRF based.

To create a VRF, we need to do:

1. create a VRF:

```
global config: ip vrf <name> rd <tag>
```

- 2) create a routing process for the VRF if we need to exchange routing info with neighbors:

```
global config: router BGP <tag>
```

3. add interface to the VRF interface set:

```
interface config: ip vrf forwarding <name>
```




---

**Note** We should not config this to gprs virtual template interface, because that is a special interface which shared by many APNs.

---

4. add a APN into the VRF:

```
APN config : vrf <name>
```



**Note**

This should be the only GPRS specific command we need. We should not put gprs vt into any VRF as mention in 3) above.

VRF based DHCP /Radius can be achieved by adding “vrf” keyword in the DHCP/Radius server command under APN and assign the associated loopback interface to the same VRF. (detail please refer to GPRS configuration guide).

Example:

```
SGSN-----GGSN-----PDN (VPN)
                               fa3/0

"use-interface" config:
-----

!
interface FastEthernet3/0
 ip address 197.0.0.1 255.0.0.0
 no ip mroute-cache
 duplex half
 no cdp enable
!

gprs access-point-list gprs
  access-point 1
  access-point-name gprs.cisco.com
  use-interface FastEthernet3/0
  exit
!

change to VRF config:
-----

!
ip vrf vpn_name1      <-----create a VRF named "vpn_name1"
 rd 100:1
ip cef                <-----must enable cef switch
!
interface FastEthernet3/0
 ip vrf forwarding vpn_name1 <----assign interface(s) to the vpn
 ip address 197.0.0.1 255.0.0.0
 no ip mroute-cache
 duplex half
 no cdp enable
!

gprs access-point-list gprs
  access-point 1
  access-point-name gprs.cisco.com
  vrf vpn_name1      <-----assign the APN to the vpn
  exit
!
```

For additional detail on configuring the VRF, refer to [www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/vpn.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/vpn.htm).



## Radius-API-Migration

This section will assist the user to perform the following:

- Understand how to change the configurations related to radius server when making a change from the GGSN Release R1.4 to GGSN Release R3.0 and upwards.
- Understand some sequence of steps which GGSN will take to authenticate a user when the server groups are configured at the APN scope as well as Global scope.

The first part gives us the simple transition example for CLI's when moving to R3.0 release. It also gives the brief reasons/advantages for making these CLI changes. At the end, have grouped the relevant new CLI's and have given sample configurations for different scenarios.

Currently on the GGSN Release R1.4, the configuration as far as the radius related commands are concerned, we do the following:

1. Have the following command under the APN:

```
radius-server 1.1.1.1
```

Or

```
radius-server 1.1.1.1 2.2.2.2 (Incase of Back-up Radius server being involved too)
```

2. Have the command at the Global GPRS level:

```
gprs default radius-server 1.1.1.1
```

3. At the Global level you would have **aaa** related commands like:

```
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
```

4. Again at the global space, the radius configurations are:

```
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server host 2.2.2.2 auth-port 1645 acct-port 1646
radius-server key lab
radius-server retransmit 3
```

So basically the issues were, we were specifying Ip address for the radius server, we cant scale to have more than 2 radius servers per APN and we had Authentication and Accounting information being sent to the same radius server only. We also didn't have a different group for the VPN radius server.

So in the R3.0 the configuration changes are as follows for the same above given configuration:

1. Under the APN you have to specify the server group:

```
aaa-group authentication <some name say xyz>
```

2. At the global GPRS level you can have the default server groups:

```
gprs default aaa-group authentication < say abc >
gprs default aaa-group accounting < say abc >
```

3. On the global place you need to define this group:

```
aaa group server radius xyz
server 1.1.1.1 auth-port 1645 acct-port 1646
server 2.2.2.2 auth-port 1645 acct-port 1646

aaa group server radius abc
server 3.3.3.3 auth-port 1645 acct-port 1646
```

4. Again on the global you need to define the method:

```
aaa authentication ppp xyz group xyz
aaa authentication ppp abc group abc
aaa authorisation network xyz group xyz
aaa authorisation network abc group abc
aaa accounting network xyz start-stop group xyz
aaa accounting network abc start-stop group abc
```

5. Again in the global radius configurations you need to define these:

```
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server host 2.2.2.2 auth-port 1645 acct-port 1646
radius-server host 3.3.3.3 auth-port 1645 acct-port 1646
radius-server key lab
radius-server retransmit 3
```

So with these changes the earlier deficiencies were removed. You also have the ability to have accounting done without authentication (for example in a transparent mode access point) etc.

**Transition Example**

Here is an example of the CLI as it exists today.

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius

gprs access-point-list gprs
  access-point 1
  access-point-name www.gprs_alcatel.fr
  radius-server 99.100.0.2
  exit

gprs default radius-server 1.2.3.4
radius-server host 99.100.0.2 auth-port 1645 acct-port 1646
radius-server host 1.2.3.4 auth-port 1645 acct-port 1646
radius-server key ggsntel
```

So with R3.0 onwards we can have

```
aaa new-model
aaa group server radius xyz
  server 99.100.0.2 auth-port 1645 acct-port 1646
aaa group server radius abc
  server 1.2.3.4. auth-port 1645 acct-port 1646

aaa authentication ppp xyz group xyz
aaa authentication ppp abc group abc
aaa authorisation network xyz group xyz
aaa authorisation network abc group abc
aaa accounting network xyz start-stop group xyz
aaa accounting network abc start-stop group abc

gprs access-point-list gprs
  access-point 1
  access-point-name www.cisco.com
  aaa-group authentication xyz
  exit
```

```

gprs default aaa-group authentication abc

radius-server host 99.100.0.2 auth-port 1645 acct-port 1646
radius-server host 1.2.3.4 auth-port 1645 acct-port 1646
radius-server key ggsntel

```

### New CLI's Added

The following CLI are being added under access-point scope.

```

aaa-group authentication|accounting <server-group-name>
aaa-accounting enable|disable

```

The following CLI are being added in global scope

```

gprs default aaa-group authentication|accounting <server-group-name>

```

The aaa-group command is used for specifying the server group that is used for authentication/accounting.

Now for authentication. If no group is specified in the apn scope, then the server group specified at the global level will be used. If that isn't also isn't there then it is mis-configuration.

For accounting purposes, if no server group is configured at the apn scope, then the server-group specified in global scope will be used. If no server group is configured in global scope, then the server group specified for authentication at the apn scope is used.

If no server group is specified for authentication the create request is rejected as the configuration is incomplete.

The aaa-accounting enable is used to enable the accounting in the transparent mode. This is when we want to do accounting without authentication.



#### Note

---

The accounting is turned on by default only in non-transparent mode.

---

### Obsoleted CLI

PLEASE NOTE THAT THE FOLLOWING CLIs WILL NOT BE SUPPORTED:

CLIs in access-point scope.

```

radius-server <ipaddress1> [<ipaddress2>]

```

CLI in global scope

```

gprs default radius-server <ipaddress1> [<ipaddress2>]

```

Sample Example Config:

At APN scope

```

gprs access-point-list gprs
  access-point 1
    access-mode non-transparent
    access-point-name www.cisco.com
    aaa-group authentication foo

```

\*\*\* The above APN config is for group foo which will

\*\*\* serve as authentication server for users of this APN.

```

access-point 2
  access-mode non-transparent
  access-point-name www.cisco1.com
  aaa-group authentication foo

```

```
aaa-group accounting foo
```

\*\*\* The above APN config is for group foo which will  
 \*\*\* serve as authentication and accounting server for  
 \*\*\* users of this APN.

```
access-point 3
  access-mode non-transparent
  access-point-name www.cisco2.com
  aaa-group authentication foo
  aaa-group accounting foo1
```

\*\*\* The above APN config is for group foo which will  
 \*\*\* serve as authentication and group foo1 will serve as  
 \*\*\* accounting server for users of this APN.

```
access-point 4
  access-mode transparent
  access-point-name www.cisco3.com
  aaa-accounting enable
  aaa-group accounting foo
```

\*\*\* The above APN config is for group foo which will  
 \*\*\* serve as accounting only.

```
access-point 5
  access-mode transparent
  access-point-name www.cisco4.com
  aaa-accounting enable
```

\*\*\* The accounting server is going to be foo3 server group  
 \*\*\* which is configured at the GPRS global scope.

```
access-point 6
  access-mode non-transparent
  access-point-name www.cisco5.com
```

\*\*\* The above APN configuration means, there will be authentication  
 \*\*\* done by the group foo2 configured at the global GPRS scope and  
 \*\*\* the accounting is done by foo3, again configured at the global  
 \*\*\* GPRS scope.

At Global GPRS space

```
gprs default aaa-group authentication foo2
gprs default aaa-group accounting foo3
```

At Global Space

```
aaa group server radius foo
  server 1.2.3.4
  server 5.6.7.8
aaa group server radius foo1
  server 10.10.0.1
aaa group server radius foo2
  server 1.2.3.4
  server 10.10.0.1
```

```

aaa group server foo3
  server 5.6.7.8
  server 10.10.0.1
  server 1.2.3.4

```

## Field Notices and Bulletins

- **Field Notices**—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at <http://www.cisco.com/warp/customer/770/index.shtml>. If you do not have a Cisco.com login account, you can find field notices at <http://www.cisco.com/warp/public/770/index.shtml>.
- **Product Bulletins**—If you have an account on Cisco.com, you can find product bulletins at <http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml>. If you do not have a Cisco.com login account, you can find product bulletins at <http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml>.
- *What's Hot for IOS Releases: Cisco IOS 12.2*—*What's Hot for IOS Releases: Cisco IOS 12.2* provides information about caveats that are related to deferred software images for Cisco IOS Release 12.2. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases: Cisco IOS 12.2* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml> or by logging in and selecting **Software Center: Cisco IOS Software: What's Hot for IOS Releases: Cisco IOS 12.2**.
- *What's New for IOS* — *What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml> or by logging in and selecting **Software Center: Cisco IOS Software: What's New for IOS**.

## Caveats for Cisco IOS Release 12.2

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)YD3.

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 on 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 & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

Because Cisco IOS Release 12.2(8)YD is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

**Table 4** Caveats Reference for Cisco IOS Release 12.2 YD

DDTS Number	Open in Release	Resolved in Release
CSCdv29286	12.2(8)YD	
CSCdx36497		12.2(8)YD2
CSCdx63665		12.2(8)YD1
CSCdy07845		12.2(8)YD2
CSCdz60229		12.2(8)YD3
CSCdz83042		12.2(8)YD3

## Open Caveats—Cisco IOS Release 12.2(8)YD3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YD3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(8)YD3.

## Resolved Caveats—Cisco IOS Release 12.2(8)YD3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YD3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz60229

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

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

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

This advisory is available at

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

- 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.

## Open Caveats—Cisco IOS Release 12.2(8)YD2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YD2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(8)YD2.

## Resolved Caveats—Cisco IOS Release 12.2(8)YD2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YD2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx36497

A block over run can occur - memory corruption - due to an error on the FE driver. The problem only occurs in very high BHCA scenarios.

There are no known workarounds.

- CSCdy07845

A router running GGSN R1.4 image c7200-g5js-mz.122-8.4 that has SNMP configured may experience a processor memory leak in the SNMP ENGINE process.

Symptoms include:

- output of “sh proc cpu” shows SNMP ENGINE process holding more and more memory without freeing the memory
- possible appearance of SYS-2-MALLOCFAIL messages in logs

Workaround: Temporarily disabling all the following OID's (sub trees)

```
1.3.6.1.4.1.9.10.48.1.1.2.2 (cgprsGtpChargingGWTable)
1.3.6.1.4.1.9.10.48.1.1.2.3 (cgprsGtpAPNTable)
1.3.6.1.4.1.9.10.48.1.2.3 (cgprsGtpGgsnStatus)
```

For general information on Troubleshooting Memory Problems, see:

<http://www.cisco.com/warp/public/63/mallocfail.shtml>

## Open Caveats—Cisco IOS Release 12.2(8)YD1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)YD1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known open caveats for Cisco IOS Release 12.2(8)YD1.

## Resolved Caveats—Cisco IOS Release 12.2(8)YD1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)YD1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx63665

A Cisco 7200 series router running Cisco Gateway GPRS Support Node (GGSN) may unexpectedly reload. The **no-partial-cdr** command is configured, but the **sgsn-change-limit** is not configured.

Workaround: Configure the `sgsn-change-limit` to any number, for example:

```
gprs charging container sgsn-change-limit 15
```

## Open Caveats—Cisco IOS Release 12.2(8)YD

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

- CSCdv29286

Cisco GGSN presently doesn't send the attributes 30, 31 and 8 which are Called Station ID (APN), Calling Station ID (MSISDN), and the Framed Ip Address (Ip Address allocated to MS) under the condition when it sends a start accounting information to the radius accounting server in case of PPP PDP session.

There are no known workarounds.

## 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 17](#)
- [Platform-Specific Documents, page 18](#)
- [Feature Modules, page 18](#)
- [Cisco IOS Software Documentation Set, page 18](#)
- [Cisco IOS Software Documentation Set, page 18](#)



## 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: Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes**



### Note

---

*Cross-Platform Release Notes for Cisco IOS Release 12.2 T* are located on Cisco.com at:  
**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Release Notes: Cisco IOS Release 12.2 T.**

---

On the Documentation CD-ROM at:

**Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes**

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

**Technical Documents**

- *Caveats for Cisco IOS Release 12.2*

As a supplement to the caveats listed in “[Caveats for Cisco IOS Release 12.2](#)” 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.

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**

- *Caveats for Cisco IOS Release 12.2 T*

As a supplement to the caveats listed in “[Caveats for Cisco IOS Release 12.2](#)” 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 on 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 & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](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)YD3 and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: 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: Cisco IOS Software: 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 5 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: Cisco IOS Software: Cisco IOS Release 12.2**

On the Documentation CD-ROM at:

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

**Table 5 Cisco IOS Release 12.2 Documentation Set**

<b>Books</b>	<b>Major Topics</b>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li>• <i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2</i></li> <li>• <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</i></li> </ul>	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 5 Cisco IOS Release 12.2 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Technologies Configuration Guide: Dial Access</i></li> <li>• <i>Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications</i></li> <li>• <i>Cisco IOS Dial Technologies Command Reference, Volume 1 of 2</i></li> <li>• <i>Cisco IOS Dial Technologies Command Reference, Volume 2 of 2</i></li> </ul>	<ul style="list-style-type: none"> <li>Dial Access</li> <li>Modem and Dial Shelf Configuration and Management</li> <li>ISDN Configuration</li> <li>Signaling Configuration</li> <li>Point-to-Point Protocols</li> <li>Dial-on-Demand Routing</li> <li>Dial Backup</li> <li>Dial Related Addressing Service</li> <li>Network Access Solutions</li> <li>Large-Scale Dial Solutions</li> <li>Cost-Control Solutions</li> <li>Internetworking Dial Access Scenarios</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>LAN Interfaces</li> <li>Serial Interfaces</li> <li>Logical Interfaces</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Configuration Guide</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i></li> <li>• <i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i></li> </ul>	<ul style="list-style-type: none"> <li>IP Addressing</li> <li>IP Services</li> <li>IP Routing Protocols</li> <li>IP Multicast</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>AppleTalk</li> <li>Novell IPX</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Apollo Domain</li> <li>Banyan VINES</li> <li>DECnet</li> <li>ISO CLNS</li> <li>XNS</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i></li> <li>• <i>Cisco IOS Voice, Video, and Fax Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Voice over IP</li> <li>Call Control Signaling</li> <li>Voice over Frame Relay</li> <li>Voice over ATM</li> <li>Telephony Applications</li> <li>Trunk Management</li> <li>Fax, Video, and Modem Support</li> </ul>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	<ul style="list-style-type: none"> <li>Packet Classification</li> <li>Congestion Management</li> <li>Congestion Avoidance</li> <li>Policing and Shaping</li> <li>Signaling</li> <li>Link Efficiency Mechanisms</li> </ul>

**Table 5** Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	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
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Mobile Wireless Configuration Guide</i></li> <li>• <i>Cisco IOS Mobile Wireless Command Reference</i></li> </ul>	General Packet Radio Service
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Terminal Services Configuration Guide</i></li> <li>• <i>Cisco IOS Terminal Services Command Reference</i></li> </ul>	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Software System Error Messages</i></li> <li>• <i>New Features in 12.2-Based Limited Lifetime Releases</i></li> <li>• <i>New Features in Release 12.2 T</i></li> <li>• <i>Release Notes</i> (Release note and caveat documentation for 12.2-based releases and various platforms)</li> </ul>	

# 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](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](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](mailto: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.

---

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

Copyright © 2002-2003  
Cisco Systems, Inc.  
All rights reserved.

