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

**December 06, 2002**

Cisco IOS Release 12.2(8)BY2

OL-3271-03

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(8)BY2. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(8)BY2, see the "Caveats for Cisco IOS Release 12.2 BY" section on page 7 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.

## 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)BY2 and includes the following sections:



## Memory Recommendations

*Table 1 Memory Recommendations for the Cisco IOS Release 12.2(8)BY2*

| Platforms | Feature Sets | Image Name | Software Image | Flash Memory Recommended | DRAM Memory Recommended | Runs From |
|---|---|---|---|---|---|---|
| **Cisco 7200 Series** | Base PDSN Standard Feature Set | PDSN 3DES+SA-ISA | c7200-c5ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Base PDSN | c7200-c5is-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | Enhanced PDSN Standard Feature Set | Enhanced PDSN 3DES+SA-ISA | c7200-c6ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Enhanced PDSN | c7200-c6is-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | Home Agent (PDSN) Standard Feature Set | Home Agent (PDSN) 3DES+SA-ISA | c7200-h1ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Home Agent (PDSN) | c7200-h1is-mz | 20 MB Flash | 512 MB DRAM | RAM |

*Table 2 Memory Recommendations for the Cisco IOS Release 12.2(8)BY1*

| Platforms | Feature Sets | Image Name | Software Image | Flash Memory Recommended | DRAM Memory Recommended | Runs From |
|---|---|---|---|---|---|---|
| **Cisco 7200 Series** | Base PDSN Standard Feature Set | PDSN 3DES+SA-ISA | c7200-c5ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Base PDSN | c7200-c5is-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | Enhanced PDSN Standard Feature Set | Enhanced PDSN 3DES+SA-ISA | c7200-c6ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Enhanced PDSN | c7200-c6is-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | Home Agent (PDSN) Standard Feature Set | Home Agent (PDSN) 3DES+SA-ISA | c7200-h1ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Home Agent (PDSN) | c7200-h1is-mz | 20 MB Flash | 512 MB DRAM | RAM |

*Table 3 Memory Recommendations for the Cisco IOS Release 12.2(8)BY*

| Platforms | Feature Sets | Image Name | Software Image | Flash Memory Recommended | DRAM Memory Recommended | Runs From |
|---|---|---|---|---|---|---|
| **Cisco 7200 Series** | Base PDSN Standard Feature Set | PDSN 3DES+SA-ISA | c7200-c5ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Base PDSN | c7200-c5is-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | Enhanced PDSN Standard Feature Set | Enhanced PDSN 3DES+SA-ISA | c7200-c6ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Enhanced PDSN | c7200-c6is-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | Home Agent (PDSN) Standard Feature Set | Home Agent (PDSN) 3DES+SA-ISA | c7200-h1ik9s-mz | 20 MB Flash | 512 MB DRAM | RAM |
| | | Home Agent (PDSN) | c7200-h1is-mz | 20 MB Flash | 512 MB DRAM | RAM |

# Supported Hardware

Cisco IOS Release 12.2(8)BY2 supports the following Cisco 7000 platforms:

- Cisco 7200 series routers (including the Cisco 7202, Cisco 7204, and Cisco 7206)
- Cisco 7200 VXR routers (including the Cisco 7204VXR and Cisco 7206VXR)

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. The following sample **show version** command output is from a router running a Cisco 7200 series software image with Cisco IOS Release 12.2(8)BY2:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (c7200-c6is-mz), Version 12.2(8)BY2, RELEASE SOFTWARE
```

# Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to *Upgrading the Cisco IOS Software Release in Cisco Routers and Modems* located at:

http://www.cisco.com/warp/public/620/6.html

# 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)BY2 supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(8)BY2 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 4 lists the feature and feature set supported by the Cisco 7200 series routers in Cisco IOS Release 12.2(8)BY2.

The table 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)BY means a feature was introduced in 12.2(8)BY. 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. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

*Table 4 Feature List by Feature Set for the Cisco 7200 Series, Part 1*

| Features | In | Software Images by Feature Sets | | | |
|---|---|---|---|---|---|
| | | PDSN 3DES+SA-ISA | Base PDSN | Enhanced PDSN 3DES+SA-ISA | Enhanced PDSN |
| Packet Data Serving Node (PDSN) | (8) | Yes | Yes | Yes | Yes |

*Table 5 Feature List by Feature Set for the Cisco 7200 Series, Part 1 (continued)*

| Features | In | Software Images by Feature Sets | | | |
|---|---|---|---|---|---|
| | | Home Agent (PDSN) 3DES+SA-ISA | Home Agent (PDSN) | | |
| Packet Data Serving Node (PDSN) | (8) | Yes | Yes | | |

# New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family of routers for Cisco IOS Release 12.2 BY.

## New Hardware Features in Cisco IOS Release 12.2(8)BY2

There are no new hardware features supported in Cisco IOS Release 12.2(8)BY2.

## New Software Features in Cisco IOS Release 12.2(8)BY2

There are no new software features supported in Cisco IOS Release 12.2(8)BY2.

## New Hardware Features in Cisco IOS Release 12.2(8)BY1

There are no new hardware features supported in Cisco IOS Release 12.2(8)BY1.

## New Software Features in Cisco IOS Release 12.2(8)BY1

There are no new software features supported in Cisco IOS Release 12.2(8)BY1.

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

There are no new hardware features supported in Cisco IOS Release 12.2(8)BY.

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

The following new software feature is supported by in Cisco IOS Release 12.2(8)BY:

## Packet Data Serving Node (PDSN)

Platforms: Cisco 7200 series routers.

Cisco PDSN is an IOS software feature that enables a Cisco 7206 router to function as a gateway between the wireless Radio Access Network (RAN) and the Internet. With Cisco PDSN enabled on a router, a stationary or roaming mobile user can access the Internet, a corporate network intranet, or Wireless Application Protocol (WAP) services. Cisco PDSN supports both Simple IP operation and Mobile IP operation.

# MIBs

## Current MIBs

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

## Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 6.

*Table 6 Deprecated and Replacement MIBs*

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

*Table 6 Deprecated and Replacement MIBs (continued)*

| Deprecated MIB | Replacement |
|---|---|
| OLD-CISCO-SYSTEM-MIB | CISCO-CONFIG-COPY-MIB |
| OLD-CISCO-TCP-MIB | CISCO-TCP-MIB |
| OLD-CISCO-TS-MIB | To be determined |
| OLD-CISCO-VINES-MIB | CISCO-VINES-MIB |
| OLD-CISCO-XNS-MIB | To be determined |

# Caveats for Cisco IOS Release 12.2 BY

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)BY2.

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

*Table 7 Caveats Reference for Cisco IOS Release 12.2 BY*

| DDTS Number | Open in Release | Resolved in Release |
|---|---|---|
| CSCdv63387 | 12.2(8)BY2 | |
| CSCdv75045 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCdv75504 | 12.2(8)BY1 | |
| CSCdw60630 | | 12.2(8)BY1 |
| CSCdx03945 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCdx55143 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCdx60192 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCdx74938 | 12.2(8)BY1 | |

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

| | | |
|---|---|---|
| CSCdx80222 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCdx86482 | | 12.2(8)BY2 |
| CSCdx90388 | 12.2(8)BY | 12.2(8)BY1 |
| CSCdy08833 | 12.2(8)BY | 12.2(8)BY1 |
| CSCdy11322 | 12.2(8)BY | 12.2(8)BY1 |
| CSCdy14130 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCdy19930 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCdy23819 | 12.2(8)BY | |
| CSCdy24978 | 12.2(8)BY | 12.2(8)BY1 |
| CSCdy34961 | | 12.2(8)BY2 |
| CSCdy35759 | 12.2(8)BY | 12.2(8)BY1 |
| CSCdy37069 | | 12.2(8)BY1 |
| CSCdy40097 | | 12.2(8)BY |
| CSCdy40189 | | 12.2(8)BY1 |
| CSCdy43978 | | 12.2(8)BY1 |
| CSCdy75288 | 12.2(8)BY1 | |
| CSCdy85867 | 12.2(8)BY1 | |
| CSCdy88090 | 12.2(8)BY1 | |
| CSCdz00198 | | 12.2(8)BY1 |
| CSCdz00743 | 12.2(8)BY1 | |
| CSCdz03252 | 12.2(8)BY1 | |
| CSCdz04509 | | 12.2(8)BY2 |
| CSCdz05272 | | 12.2(8)BY1 |
| CSCdz12036 | 12.2(8)BY1 | |
| CSCdz19118 | | 12.2(8)BY2 |
| CSCdz21896 | | 12.2(8)BY2 |
| CSCdz23611 | | 12.2(8)BY2 |
| CSCdz32147 | | 12.2(8)BY2 |
| CSCdz38529 | | 12.2(8)BY2 |
| CSCin06371 | | 12.2(8)BY2 |
| CSCin10386 | 12.2(8)BY,<br>12.2(8)BY1 | |
| CSCin15071 | | 12.2(8)BY1 |
| CSCin15149 | 12.2(8)BY | 12.2(8)BY1 |
| CSCin16292 | 12.2(8)BY | 12.2(8)BY1 |

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

| | | |
|---|---|---|
| CSCin18138 | | 12.2(8)BY1 |
| CSCin19975 | 12.2(8)BY1 | |
| CSCin22446 | 12.2(8)BY1 | |
| CSCin22974 | | 12.2(8)BY2 |
| CSCin23552 | | 12.2(8)BY2 |
| CSCin23557 | | 12.2(8)BY2 |
| CSCin23921 | | 12.2(8)BY2 |
| CSCin24256 | | 12.2(8)BY2 |
| CSCin25669 | | 12.2(8)BY2 |

# Open Caveats—Cisco IOS Release 12.2(8)BY2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)BY2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv63387

  PDSN drops packets at moderate traffic conditions, and hence NDR throughput is very low when compared with the Max.throughput. This degradation is observed when AHDLC fragmentation is configured on the PCF.

  There are no known workarounds.

# Resolved Caveats—Cisco IOS Release 12.2(8)BY2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)BY2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx86482

  Point-to-Point Tunneling Protocol (PPTP) tunneling may not function, and data sent by a PPTP network server (PNS) may have invalid PPTP headers.

  This symptom is observed after a virtual private dial-up network (VPDN) session comes up.

  There are no known workarounds.

- CSCdy34961

  Spurious memory access made at vpdn_sss_perform_dynamic_bind. This occurs on a c7200 router while testing PPTP with SSS.

  There are no known workarounds.

- CSCdz04509

  On a c7200 running Cisco IOS 12.2B-based PDSN, the object cCdmaPppRenegConnectionsAborted may not increment if the foll. scenarios of aborted PPP calls occur:

  1. A TERMREQ received during PPP renegotiation

  2. A RRQ with Lifetime=0 received during PPP renegotiation

  The problem has been fixed in 12.2(8)BY2 release.

  There are no known workarounds.

- CSCdz19118

  When ping is made over MIP flow with reverse tunnel and compression, downstream packets to MN are dropped at PDSN.

  Workaround: Disable CEF and ping goes through over the flow.

- CSCdz21896

  When PDSN is configured under Controller-Member architecture While opening sessions the member might crash.

  The PDSN might crash only when it is configured as a member under Controller-Member clustering.

  Workaround: Do not configure the PDSN as a member under Controller-Member clustering.

- CSCdz23611

  For MIP with header compression and CEF enabled, the compression counters are incorrect when TCP packets are sent over the MIP flow.

  Workaround: Disable CEF and the header compression counters are working fine.

- CSCdz32147

  While opening and closing MOIP sessions using 6500 mwam pdsn, HA is reloaded when “show ip mobile tunnel” command is issued.

  There are no known workarounds.

- CSCdz38529

  Accounting for VPDN sessions is excluding the PPP STATION (FF03) bytes from packets to PDSN and packets from LNS to PDSN.

  PDSN is not accounting the PPP STATION bytes (2 bytes) in packets received from Mobile and Packets received from the LNS.

  There are no known workarounds.

- CSCin06371

  The SNMP query to cssgStatsObjects object-group return zero for the objects listed below:

  ```
  cssgStatsLoginAttempts
  cssgStatsLoginsSuccessful
  cssgStatsActiveSessions
  cssgStatsActiveHosts
  cssgStatsActiveServices
  cssgStatsPODs
  ```

  The above mentioned problem can be noticed under all conditions as the feature has not been implemented yet.

  The problem has been fixed and code was committed to c6400_pi7, ssg_oxygen_pi branches.

  There are no known workarounds.

- CSCin22974

  On a c7200 running Cisco IOS 12.2B-based PDSN, when a PPP negotiation fails due to LCP timeout, cCdmaPppLcpFailures counters don't get incremented.

  The problem has been fixed in 12.2(8)BY2 release.

  There are no known workarounds.

- CSCin23552

  On a c7200 running Cisco IOS 12.2B-based PDSN, when a PPP session, for Simple IP service, comes up without IP address, neither the cCdmaPppConnectionSuccesses nor cCdmaPppConnectionFailures counter get incremented.

  On the completion IPCP negotiation, if one of Service Selection Criterias is not met, RP and PPP sessions tear down. In this scenario, neither the cCdmaPppConnectionSuccesses nor cCdmaPppConnectionFailures counter won't get incremented.

  The problem has been fixed in 12.2(8)BY2 release. The fix counts the PPP session as successfully negotiated as the actual failure is that one of the Service Selection Criterias (explained in PDSN PFS, Section 10) is not met.

  There are no known workarounds.

- CSCin23557

  On a c7200 running Cisco IOS 12.2B-based PDSN, when a PPP negotiation fails during IPCP phase because of IP address shortage, the cCdmaPppIpcpFailures counter doesn't get incremented.

  This condition occurs on virtual-template, the "ppp ipcp address required" option is configured.

  When the above command is configured, if IP address shortage happens, PPP will get terminated.

  The problem has been fixed in 12.2(8)BY2 release.

  There are no known workarounds.

- CSCin23921

  The accounting for VSA attributes Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets and Acct-Output-Packets is incorrect between 2 accounting stops. The packets/bytes are counted only between the last accounting start and accounting stop. The packets/bytes between last accounting stop and accounting start is not counted.

  Mobile moves to dormant state and data is pumped during that time. When the mobile moves to active state, the number of packets accounted are between the last accounting start and accounting stop, instead of between 2 accounting stops.

  There are no known workarounds.

- CSCin24256

  In CISCO PDSN, in some scenarios the visitor is getting deleted without decrementing the visitor count of FA. So, the visitor count will be more than the active vistors.

  There are no known workarounds.

- CSCin25669

  After the execution of the config command for resizing the failure-history table, cCdmaFailHistInfo table becomes empty:

  ```
  cdma pdsn failure-history <table-size>
  ```

  There are no known workarounds.

# Open Caveats—Cisco IOS Release 12.2(8)BY1

This section documents possible unexpected behavior by Cisco IOS Release 12.2(8)BY1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv75504

  When a Mobile IP session is opened, and packets are sent through the tunnel, the **show interface tunnel X accounting** command (on the Mobile IP tunnel) does not show any protocol based accounting information.

  There are no known workarounds.

- CSCdv75045

  Occasional packet drops occur when a downstream sweep ping is executed, and when there are more than 8000 Mobile IP sessions hosted on the PDSN.

  There are no known workarounds.

- CSCdx03945

  Adding hex strings that are exactly 31 bytes in length to the following directive will incorrectly set the key value:

  ```
  ip mobile secure host 10.0.0.1 spi 100 key hex 12345678901234567890123456789O1
  ```

  A workaround is to make sure the value is exactly 32 bytes in length.

- CSCdx55143

  On the Cisco PDSN, a quota request is sent for a non-prepaid user if it is opened on a prepaid session. A quota request should not be sent for a non-prepaid user if the user registers over an already existing session that has an active prepaid flow.

  A workaround is to register the non-prepaid user over a new session.

- CSCdx60192

  If IP fragmentation is enabled on the PCF, and AHDLC fragment size is greater than this value, then packets from the MN with an AHDLC fragment size that is less than the MTU configured on the PCF will be processed in the fastpath in the PDSN. This will cause AHDLC FCS errors.

  A workaround is to remove any IP fragmentation on the PCF unless it is absolutely necessary.

- CSCdx74938

  After opening 10,000 Simple IP sessions, and PPP renegotiation is initiated, those sessions will go down.

  There are no known workarounds.

- CSCdx80222

  On the Cisco PDSN, a MobileIP flow will not come up if IPCP renegotiation is initiated by a MN after the session is up.

  There are no known workarounds.

- CSCdy14130

  PDSN reloads when you simultaneously close compression sessions and issue the **show compress detail-ccp** command.

  As a workaround, do not issue **show compress detail-ccp** command while closing compression sessions.

- CSCdy19930

  On the Cisco PDSN, malloc failures are observed (with periodic accounting update 1), while mobiles connect and disconnect simultaneously.

  A workaround is to disable periodic accounting update 1, or enter much higher values of periodic accounting intervals.

- CSCdy75288

  PPP data packets received at the PDSN from the mobile get switched to the Pi interface, even if the flow for the corresponding mobile is not yet created. This causes them to remain unaccounted for.

  This problem happens only when the RP session has been established between the PCF and the PDSN, and an ahdlc channel has been allocated to the mobile. Thus, it occurs only for a short period of time before the flow gets created, or the flow fails to get established.

  There are no known workarounds.

- CSCdy85867

  When 20000 sessions are open and PPP is renegotiated over them at a high rate—and you then close down of the sessions—a few sessions on the PDSN do not get closed successfully. Apparently, IPCP is continuously trying to send out Config Request packets, and these packets never go out of the box.

  There are no known workarounds.

- CSCdy88090

  On the PDSN, the **clear cdma pdsn statistics** command may not clear the AHDLC related statistics.

  There are no known workarounds.

- CSCdz00743

  On the PDSN, the following MIB objects may return NULL values, even though the corresponding service type flow actually fails to come up when underlying PPP session is UP.

  - cCdmaFlowSimpleIpFailures
  - cCdmaFlowMobilIpFailures
  - cCdmaFlowProxyIpFailures
  - cCdmaFlowVpdnFailures

  There are no known workarounds.

- CSCdz03252

  On the PDSN, the following MIB objects may not increment even though I/O memory is locked up, and malloc failures appear.

  - cCdmaAhdlcMemDropPktsDec
  - cCdmaAhdlcMemDropPktsEnc

  There are no known workarounds.

- CSCdz12036

  Running a Cisco PDSN at stress conditions causes sessions flapping; additionally, the PPP renegotiation success and failure counters do not tally with the total renegotiation counter.

  There is no work around; however, this condition only occurs during stress conditions.

- CSCin10386

  While opening 8000 sessions with one Mobile IP flow each, the MobileIp flows count occasionally becomes greater than the session count.

  There are no known workarounds.

- CSCin19975

  On the PDSN, PPP renegotiation may not be initiated by the PDSN during the second PDSN-to-PDSN handoff when the mobile moves between the same PDSNs.

  There are no known workarounds.

- CSCin22446

  After disabling the ip route-cache (**no ip route-cache**), and enabling it again

  with the **ip route-cache cef** command on the PDSN virtual-template, the CEF is not enabled on the vaccess.

  There are no known workarounds.

# Resolved Caveats—Cisco IOS Release 12.2(8)BY1

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(8)BY1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw60630

  When a dormant handoff takes place on the PDSN, the PDSN does not send Release Indicator (F13 Accounting Attribute) to the radius server. This problem only occurs when the **cdma pdsn accounting send start-stop** command is configured on the PDSN.

  As a workaround, for dormant handoffs, do not configure the **cdma pdsn accounting send start-stop** command.

- CSCdx90388

  Opening Mobile IP sessions at a high rate (>50cps) can cause a session to become stuck in opening state.

  The workaround is to use a lower call setup rate when opening Mobile IP sessions (~20cps).

- CSCdy08833

  After opening of Mobile IP sessions, BADSHARE Tracebacks were observed while reloading the PDSN.

  There are no known workarounds.

- CSCdy11322

  When precloning is configured, and the PDSN generates a proxy MIP request, that request fails if compression attributes are returned from AAA.

  A workaround is to disable the configuration for precloning.

- CSCdy24978

  On the Cisco PDSN, at high call setup rates (greater than 150 cps), the cluster may drop new calls. Adding more members to the cluster does not improve the call setup rates linearly.

  There is no workaround

- CSCdy35759

  When opening and closing PDSN sessions, the PPP CHAP attempts and success counters may not match in the output of the **show cdma pdsn statistics** command.

  There are no known workarounds.

- CSCdy37069

  On a router equipped with a hardware compression component, the PDSN reloads when “compress stac” is configured (instead of “compress stac software”) on a PDSN virtual template interface, and there is no user session utilizing that virtual template.

  As a workaround, do not configure PPP hardware payload compression on a virtual template interface when the virtual template is to be used for PDSN CDMA. If compression is needed on a virtual interface, use any of the following.

  a. specify software compression in the configuration command, or
  b. establish a user session before configuring compression, or
  c. remove the compression hardware from the router.

- CSCdy40189

  The Cluster Controller sends two cCdmaClusterMemberStatusChange traps when the PDSN member status changes.

  There is no workaround because the problem could not be reproduced.

- CSCdy43978

  Malloc failures are observed while sending UP stream fragmented traffic through 20,000 Mobile IP Sessions. These failures are due to high packet rate; memory is recovered once the traffic is stopped.

  A workaround is to set the maximum sessions on the PDSN to 8000.

- CSCdz00198

  A Cisco 7200 router that is running 12.2.1a.XC version of the PDSN solution, frequently reloads. This bug is a duplicate of CSCdw50718.

  There are no known workarounds.

- CSCdz05272

  While displaying **show aaa sessions**, the PDSN crashed and auto-reloaded.

  This bug is a duplicate of CSCdu58983.

  There are no known workarounds.

- CSCin15071

  The SNMP query on the cCdmaAffectedAddress object on the PDSN cluster member returns a null string.

  There is no workaround because the problem could not be reproduced.

- CSCin15149

  During mobile poweroff, before IPCP is up, the proxy registration entry is not getting deleted. At this point the user cannot perform proxy registration again.

  A workaround is to delete the proxy registration, allowing the proxy flow to be opened.

- CSCin16292

  In a Cisco PDSN, the following MIB variables will return incorrect values:

  - cmiSecAlgorithmType and cmiSecAlgorithmMode will not support HMAC configurations, and will only return a value of “Other” (1).
  - faVisitorRegIDHigh variable may show negative values.
  - maAdvConfigTable will not return all the Vaccess details.

  The following two variables are not supported, and will always return a “FALSE” value.

  - faIsBusy
  - faRegistrationRequired

  There are no known workarounds.

- CSCin18138

  Some of the PPP Setup, RP Registration, Session failure and Clustering-related MIB counters may not return correct values on snmp query.

  There are no known workarounds.

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

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

- CSCdv75045

  Occasional packet drops are observed when downstream sweep ping is executed, when there are 8000 MoIP sessions hosted on the SW AHDLC engine.

  There are no known workarounds.

- CSCdx03945

  Do not add hex strings that are exactly 31 bytes in length to the following directive:

  ```
  ip mobile secure host 10.0.0.1 spi 100 key hex 12345678901234567890123456789O1
  ```

  This will incorrectly set the key value. Make sure the value is *exactly* 32 bytes in length.

  There are no known workarounds.

- CSCdx55143

  Quota request should not be sent for a non-prepaid user if the user registers over an already existing session which has a prepaid flow active.

  Workaround: Register the non-prepaid user over a new session.

- CSCdx60192

  When using Cisco PDSN image, if IP fragmentation is enabled on the PCF, and AHDLC fragment size is greater than this, then packets from the MN with AHDLC fragment size lesser than the MTU configured on the PCF will be processed in the fastpath in the PDSN, and this will cause AHDLC FCS errors.

  Workaround: Remove any IP fragmentation on the PCF unless absolutely necessary.

- CSCdx80222

  MobileIP flow will not come up, if IPCP renegotiation is initiated by MN after the session is up.

  There are no known workarounds.

- CSCdx90388

  While opening MOIP sessions, one session got stuck in opening state. Opening MOIP sessions at a high rate (>50cps)caused one session to become stuck in opening state. The MoIP registration packet may be lost for any reason which will cause this problem.

  Workaround: Use a lower call setup rate when opening MOIP sessions (~20cps)

- CSCdy08833

  BADSHARE Tracebacks observed while reloading PDSN. This occurs while reloading after creating MOIP Sessions

  There are no known workarounds.

- CSCdy11322

  When precloned virtual-access interfaces are used, the type of the virtual access may not be set correctly. This can cause various problems from the output of the **show int virtual-access** not showing how the virtual-access is being used to functional problems for PDSN.

  When PDSN generates a proxy MIP request, that request fails if compression attributes are returned from AAA and precloning is configured.

  Workaround: Deconfigure precloning.

- CSCdy14130

  PDSN unexpectedly reloads when we close compression sessions and issue the **show compress detail-ccp** command at the same time.

  Workaround: Do not issue the **show compress detail-ccp** command while closing compression sessions.

- CSCdy19930

  Malloc failures observed with periodic accounting update 1, while Mobiles connect and disconnect simultaneously.

  The following conditions are known to cause this problem:

  - Open and close 2000 MOIP and 2000 SIP Sessions. Active time for each session is 120 sec, and inactive time is 180 seconds.
  - Set Periodic accounting update as 1
  - Repeat the above test 10 times.
  - Malloc failures observed on PDSN

  Workaround: Disable Periodic accounting update 1

  Alternative workaround: Use much higher values of periodic accounting intervals.

- CSCdy23819

  Using private addresses A and B, if we register two MNs, one with care-of address as A, and its home address as B and the other with care-of address as B, and its home address as A, then the HA crashes when processing the second registration.

  Workaround: Since this is possible only when both the MNs and the PDSNs are in the same, one workaround is to use only public care-of addresses in both the PDSNs.

- CSCdy24978

  At high call setup rates (greater than 150 cps), the cluster may drop new calls.

  Call setup rate seen with the addition of more members to the cluster does not improve linearly. At call rates higher than 150 cps per cluster, the cluster exhibits call drops.

  There are no known workarounds.

- CSCdy35759

  When opening and closing PDSN sessions, the PPP CHAP attempts and success counters may not match in the output of the show cdma pdsn statistics command.

  There are no workarounds.

- CSCin10386

  While Opening 8000 sessions with one mobileIP flow each, sometimes the mobileIp flows count becomes greater than session count.

  There are no known workarounds.

- CSCin15149

  During poweroff close before IPCP up, the proxy registration entry is not getting deleted. So, the user cannot perform proxy registration again.

  Workaround: Delete the proxy registration, then proxy flow can be opened.

- CSCin16292

  In a Cisco 12.2B based PDSN, the following MIB variables will return incorrect values:

  - cmiSecAlgorithmType and cmiSecAlgorithmMode will not support HMAC configs. It will return only value as Other(1).
  - faVisitorRegIDHigh variable may show values in Negative.
  - faIsBusy
  - faRegistrationRequired. The above two variables are not supported and will always return as FALSE.
  - maAdvConfigTable will not return all the Vaccess details.

  There are no known workarounds.

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

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

- CSCdy40097

  The Cisco PDSN drops packets which are compressed with TCP header compression, Address Control Field Compression (ACFC), and Protocol Field Compression (PFC).

  Workaround: Disable one of these compression schemes

  Alternative workaround: Configure **no ip route-cache** on the virtual template, and **no ip cef** in the global configuration.

# Related Documentation

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

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

Use these release notes with these documents:


- Release-Specific Documents, page 20
- Platform-Specific Documents, page 21
- Feature Modules, page 21
- Cisco IOS Software Documentation Set, page 22


## 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**

  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(8)BY2*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 BY" in these release notes, see *Caveats for Cisco IOS Release 12.2* and *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 and Cisco IOS Release 12.2 T.

  On Cisco.com at:

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

# Platform-Specific Documents

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

- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7206 Installation and Configuration Guide*
- *Cisco 7204 Installation and Configuration Guide*
- *Quick Reference for Cisco 7204 Installation*
- *Cisco 7202 Installation and Configuration Guide*
- *Quick Start Guide Cisco 7100 Series VPN Router*
- *Cisco 7010 User Guide*
- *Cisco 7000 User Guide*
- *Cisco 7000 Hardware Installation and Maintenance*

  On Cisco.com at:

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

  On the Documentation CD-ROM at:

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

# Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(8)BY2 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**

# Feature Navigator

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

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

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

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

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

# Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

## Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com at:

**Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Configuration Guides and Command References**

On the Documentation CD-ROM at:

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

## Cisco IOS Release 12.2 Documentation Set Contents

Table 8 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

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

On Cisco.com at:

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

On the Documentation CD-ROM at:

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

*Table 8 Cisco IOS Release 12.2 Documentation Set*

| Books | Major Topics |
|---|---|
| • Cisco IOS Configuration Fundamentals Configuration Guide<br>• Cisco IOS Configuration Fundamentals Command Reference | Cisco IOS User Interfaces<br>File Management<br>System Management |
| • Cisco IOS Bridging and IBM Networking Configuration Guide<br>• Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2<br>• Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2 | Transparent Bridging<br>SRB<br>Token Ring Inter-Switch Link<br>Token Ring Route Switch Module<br>RSRB<br>DLSW+<br>Serial Tunnel and Block Serial Tunnel<br>LLC2 and SDLC<br>IBM Network Media Translation<br>SNA Frame Relay Access<br>NCIA Client/Server<br>Airline Product Set<br>DSPU and SNA Service Point<br>SNA Switching Services<br>Cisco Transaction Connection<br>Cisco Mainframe Channel Connection<br>CLAW and TCP/IP Offload<br>CSNA, CMPC, and CMPC+<br>TN3270 Server |
| • Cisco IOS Dial Technologies Configuration Guide: Dial Access<br>• Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications<br>• Cisco IOS Dial Technologies Command Reference, Volume 1 of 2<br>• Cisco IOS Dial Technologies Command Reference, Volume 2 of 2 | Dial Access<br>Modem and Dial Shelf Configuration and Management<br>ISDN Configuration<br>Signaling Configuration<br>Point-to-Point Protocols<br>Dial-on-Demand Routing<br>Dial Backup<br>Dial Related Addressing Service<br>Network Access Solutions<br>Large-Scale Dial Solutions<br>Cost-Control Solutions<br>Internetworking Dial Access Scenarios |
| • *Cisco IOS Interface Configuration Guide*<br>• *Cisco IOS Interface Command Reference* | LAN Interfaces<br>Serial Interfaces<br>Logical Interfaces |
| • Cisco IOS IP Configuration Guide<br>• Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services<br>• Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols<br>• Cisco IOS IP Command Reference, Volume 3 of 3: Multicast | IP Addressing<br>IP Services<br>IP Routing Protocols<br>IP Multicast |
| • Cisco IOS AppleTalk and Novell IPX Configuration Guide<br>• Cisco IOS AppleTalk and Novell IPX Command Reference | AppleTalk<br>Novell IPX |

*Table 8 Cisco IOS Release 12.2 Documentation Set (continued)*

| Books | Major Topics |
|---|---|
| • Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide<br>• Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference | Apollo Domain<br>Banyan VINES<br>DECnet<br>ISO CLNS<br>XNS |
| • Cisco IOS Voice, Video, and Fax Configuration Guide<br>• *Cisco IOS Voice, Video, and Fax Command Reference* | Voice over IP<br>Call Control Signaling<br>Voice over Frame Relay<br>Voice over ATM<br>Telephony Applications<br>Trunk Management<br>Fax, Video, and Modem Support |
| • Cisco IOS Quality of Service Solutions Configuration Guide<br>• *Cisco IOS Quality of Service Solutions Command Reference* | Packet Classification<br>Congestion Management<br>Congestion Avoidance<br>Policing and Shaping<br>Signaling<br>Link Efficiency Mechanisms |
| • Cisco IOS Security Configuration Guide<br>• *Cisco IOS Security Command Reference* | AAA Security Services<br>Security Server Protocols<br>Traffic Filtering and Firewalls<br>IP Security and Encryption<br>Passwords and Privileges<br>Neighbor Router Authentication<br>IP Security Options<br>Supported AV Pairs |
| • Cisco IOS Switching Services Configuration Guide<br>• Cisco IOS Switching Services Command Reference | Cisco IOS Switching Paths<br>NetFlow Switching<br>Multiprotocol Label Switching<br>Multilayer Switching<br>Multicast Distributed Switching<br>Virtual LANs<br>LAN Emulation |
| • Cisco IOS Wide-Area Networking Configuration Guide<br>• Cisco IOS Wide-Area Networking Command *Reference* | ATM<br>Frame Relay<br>SMDS<br>X.25 and LAPB |
| • Cisco IOS Mobile Wireless Configuration Guide<br>• Cisco IOS Mobile Wireless Command Reference | General Packet Radio Service |

*Table 8 Cisco IOS Release 12.2 Documentation Set (continued)*

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

# Obtaining Documentation

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

## World Wide Web

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

## Documentation CD-ROM

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

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

## Documentation Feedback

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

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

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

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

We appreciate your comments.

# Obtaining Technical Assistance

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

## Cisco.com

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

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

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

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

http://www.cisco.com

# Technical Assistance Center

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

## Contacting TAC by Using the Cisco TAC Website

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

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

## Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 20.