Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 XB

January 13, 2004

Cisco IOS Release 12.2(2)XB15

OL-1837-09

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(2)XB15. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(2)XB15, see the "Caveats for Cisco IOS Release 12.2 XB" 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.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback or go to the following URL to give us your feedback:
http://www.cisco.com/warp/public/732/docsurvey/rtg/ to give us your feedback .

Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 4
- MIBs, page 6
- Important Notes, page 7
- Caveats for Cisco IOS Release 12.2 XB, page 7

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

- Related Documentation, page 37
- Obtaining Documentation, page 43
- Obtaining Technical Assistance, page 44

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(2)XB15 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 Memory Recommendations for the Cisco IOS Release 12.2(2)XB

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200 Series	IP Standard Feature Set	IP	c7200-is-mz	16 MB Flash	128 MB DRAM	RAM
	Enterprise Standard Feature Set	Enterprise	c7200-js-mz	16 MB Flash	128 MB DRAM	RAM

Supported Hardware

Cisco IOS Release 12.2(2)XB15 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 4.

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(2)XB15:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (c7200-is-mz), Version 12.2(2)XB15, 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(2)XB15 supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(2)XB15 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 2 lists the feature and feature set supported by the Cisco 7200 series routers in Cisco IOS Release 12.2(2)XB.

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, (2)XB3 means a feature was introduced in 12.2(2)XB3. 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 2 Feature List by Feature Set for the Cisco 7200 Series, Part 1

Features	In	Software Images by Feature Sets			
		IP	Enterprise		
IP Routing					
Survivable Remote Site Telephony	(2)	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 XB.

New Hardware Features in Cisco IOS Release 12.2(2)XB15

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB15.

New Software Features in Cisco IOS Release 12.2(2)XB15

There are no new software features supported in Cisco IOS Release 12.2(2)XB15.

New Hardware Features in Cisco IOS Release 12.2(2)XB14

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB14.

New Software Features in Cisco IOS Release 12.2(2)XB14

There are no new software features supported in Cisco IOS Release 12.2(2)XB14.

New Hardware Features in Cisco IOS Release 12.2(2)XB7

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB7.

New Software Features in Cisco IOS Release 12.2(2)XB7

There are no new software features supported in Cisco IOS Release 12.2(2)XB7.

New Hardware Features in Cisco IOS Release 12.2(2)XB6

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB6.

New Software Features in Cisco IOS Release 12.2(2)XB6

There are no new software features supported in Cisco IOS Release 12.2(2)XB6.

New Hardware Features in Cisco IOS Release 12.2(2)XB5

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB5.

New Software Features in Cisco IOS Release 12.2(2)XB5

There are no new software features supported in Cisco IOS Release 12.2(2)XB5.

New Hardware Features in Cisco IOS Release 12.2(2)XB4

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB4.

New Software Features in Cisco IOS Release 12.2(2)XB4

There are no new software features supported in Cisco IOS Release 12.2(2)XB4.

New Hardware Features in Cisco IOS Release 12.2(2)XB3

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB3.

New Software Features in Cisco IOS Release 12.2(2)XB3

There are no new software features supported in Cisco IOS Release 12.2(2)XB3.

New Hardware Features in Cisco IOS Release 12.2(2)XB2

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB2.

New Software Features in Cisco IOS Release 12.2(2)XB2

There are no new software features supported in Cisco IOS Release 12.2(2)XB2.

New Hardware Features in Cisco IOS Release 12.2(2)XB

There are no new hardware features supported in Cisco IOS Release 12.2(2)XB.

New Software Features in Cisco IOS Release 12.2(2)XB

The following new software feature is supported by in Cisco IOS Release 12.2(2)XB:

Survivable Remote Site Telephony

Platforms: Cisco 7200 series routers.

The Survivable Remote Site (SRS) Telephony feature, under the IP Telephony services umbrella, provides the Cisco CallManager with fallback support for the Cisco IP phones attached to the Cisco router on your local Ethernet. The SRS Telephony feature enables the routers to provide call handling support for the Cisco IP phones when the Cisco IP phones lose connection to the remote primary, secondary, or tertiary Cisco CallManager or when the WAN connection is down.

Cisco CallManager 3.0 supports Cisco IP phones at remote sites attached to Cisco branch office multiservice routers across the WAN. Prior to the SRS Telephony feature, when the WAN connection between the remote branch office router and the Cisco CallManager failed or connectivity with the Cisco CallManager was lost for some reason, the Cisco IP phones at the branch office became unusable for the duration of the failure. The SRS Telephony feature overcomes this problem and enables the basic features of the Cisco IP phones by providing call-handling support on the branch office router for its attached Cisco IP phones. The system automatically detects the failure and uses the Simple Network Auto Provisioning (SNAP) technology to autoconfigure the branch office router to provide call processing for the local Cisco IP phones. When the WAN link or connection to the primary Cisco CallManager is restored, call-handling capabilities for the Cisco IP phones switch back to the primary Cisco CallManager. During a failure when SRS Telephony feature is enabled, the Cisco IP phone displays a message to inform you that the Cisco IP phones are in the Cisco CallManager fallback mode and are able to perform limited functions.

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

Table 3 Deprecated and Replacement MIBs (continued)

Deprecated MIB	Replacement
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(2)XB2 that can apply to the Cisco 7000 family.

Cisco IOS Release 12.2(2)XB2

Cisco 7200 images are not orderable in Cisco IOS Release 12.2(2)XB2. However, the Cisco 7200 images can be used when downloaded from Cisco.com.

Caveats for Cisco IOS Release 12.2 XB

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(2)XB15.

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/.

Because Cisco IOS Release 12.2(2)XB is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

Table 4 Caveats Reference for Cisco IOS Release 12.2 XB

DDTS Number	Open in Release	Resolved in Release
CSCdr47232		12.2(2)XB4
CSCdr81193		12.2(2)XB5
CSCdr85436		12.2(2)XB4
CSCdr93141		12.2(2)XB4
CSCds36738		12.2(2)XB5
CSCdt55987	12.2(2)XB	
CSCdt63321		12.2(2)XB4
CSCdu14530		12.2(2)XB5
CSCdu19432		12.2(2)XB4
CSCdu35843		12.2(2)XB4
CSCdu36862		12.2(2)XB4
CSCdu40402		12.2(2)XB4
CSCdu40615		12.2(2)XB4
CSCdu43689		12.2(2)XB4
CSCdu64847		12.2(2)XB4
CSCdu67010		12.2(2)XB4
CSCdu74728		12.2(2)XB4
CSCdu84692		12.2(2)XB4
CSCdu86243		12.2(2)XB4
CSCdv01412		12.2(2)XB4
CSCdv01555		12.2(2)XB4
CSCdv02732		12.2(2)XB4
CSCdv03076		12.2(2)XB4
CSCdv03689		12.2(2)XB4
CSCdv04999		12.2(2)XB4
CSCdv13634		12.2(2)XB4
CSCdv20977		12.2(2)XB4
CSCdv19031		12.2(2)XB4

Table 4 Caveats Reference for Cisco IOS Release 12.2 XB (continued)

CSCdv19928		12.2(2)XB4
CSCdv21918		12.2(2)XB7
CSCdv29468		12.2(2)XB4
CSCdv26709		12.2(2)XB4
CSCdv33270		12.2(2)XB4
CSCdv33313		12.2(2)XB4
CSCdv34768		12.2(2)XB4
CSCdv38563	12.2(2)XB4	12.2(2)XB5
CSCdv40116		12.2(2)XB4
CSCdv40729		12.2(2)XB4
CSCdv41871		12.2(2)XB4
CSCdv43136		12.2(2)XB4
CSCdv43856		12.2(2)XB4
CSCdv54127		12.2(2)XB5
CSCdv54349		12.2(2)XB4
CSCdv62649		12.2(2)XB4
CSCdv64668		12.2(2)XB4
CSCdv66747		12.2(2)XB5
CSCdv67009		12.2(2)XB4
CSCdv71454		12.2(2)XB5
CSCdv76649		12.2(2)XB4
CSCdv78693		12.2(2)XB4
CSCdv79210		12.2(2)XB4
CSCdv83040		12.2(2)XB4
CSCdv83402		12.2(2)XB4
CSCdv87754		12.2(2)XB4
CSCdw00019		12.2(2)XB4
CSCdw00924		12.2(2)XB5
CSCdw01726		12.2(2)XB4
CSCdw02945		12.2(2)XB4
CSCdw06038		12.2(2)XB5
CSCdw06322		12.2(2)XB4
CSCdw09542		12.2(2)XB4
CSCdw11765		12.2(2)XB4
CSCdw13432		12.2(2)XB4
CSCdw18785		12.2(2)XB4
CSCdw23836		12.2(2)XB4

Table 4 Caveats Reference for Cisco IOS Release 12.2 XB (continued)

CSCdw25746		12.2(2)XB4
CSCdw28786		12.2(2)XB4
CSCdw30994		12.2(2)XB4
CSCdw35046		12.2(2)XB4
CSCdw35930		12.2(2)XB4
CSCdw39083		12.2(2)XB5
CSCdw43862		12.2(2)XB4
CSCdw45584		12.2(2)XB5
CSCdw46065		12.2(2)XB4
CSCdw53071		12.2(2)XB4
CSCdw53243		12.2(2)XB4
CSCdw58199		12.2(2)XB5
CSCdw62064		12.2(2)XB5
CSCdw62969		12.2(2)XB4
CSCdw65903		12.2(2)XB3, 12.2(2)XB4
CSCdw66251		12.2(2)XB4
CSCdw68658	12.2(2)XB4	
CSCdw68757		12.2(2)XB5
CSCdw75532		12.2(2)XB5
CSCdw77524	12.2(2)XB4	
CSCdw80521		12.2(2)XB5
CSCdw80646		12.2(2)XB5
CSCdw80687		12.2(2)XB5
CSCdw85178		12.2(2)XB5
CSCdw89455		12.2(2)XB5
CSCdw91279		12.2(2)XB5
CSCdx02102		12.2(2)XB5
CSCdx02525		12.2(2)XB5
CSCdw00055		12.2(2)XB7
CSCdx03583		12.2(2)XB5
CSCdx05704		12.2(2)XB5
CSCdx08078		12.2(2)XB5
CSCdx08525		12.2(2)XB5
CSCdx09410		12.2(2)XB5
CSCdx11607		12.2(2)XB5
CSCdx20135		12.2(2)XB5
CSCdx22886		12.2(2)XB5

Table 4 Caveats Reference for Cisco IOS Release 12.2 XB (continued)

CSCdx26331		12.2(2)XB5
CSCdx33166		12.2(2)XB7
CSCdx40546		12.2(2)XB5
CSCdx41547		12.2(2)XB5
CSCdx46375		12.2(2)XB5
CSCdx76632		12.2(2)XB14, 12.2(2)XB15
CSCdx93324		12.2(2)XB7
CSCdy05296		12.2(2)XB7
CSCdy14689		12.2(2)XB7
CSCdy16593		12.2(2)XB7
CSCea19885		12.2(2)XB14, 12.2(2)XB15
CSCea27536		12.2(2)XB14, 12.2(2)XB15
CSCea32240		12.2(2)XB14, 12.2(2)XB15
CSCea33065		12.2(2)XB14, 12.2(2)XB15
CSCea36231		12.2(2)XB14, 12.2(2)XB15
CSCea46342		12.2(2)XB14, 12.2(2)XB15
CSCea51030		12.2(2)XB14, 12.2(2)XB15
CSCea51076		12.2(2)XB14, 12.2(2)XB15
CSCea54851		12.2(2)XB14, 12.2(2)XB15
CSCeb78836		12.2(2)XB14, 12.2(2)XB15
CSCec87533		12.2(2)XB15
CSCin00405	12.2(2)XB4	
CSCin03065		12.2(2)XB5
CSCin06313		12.2(2)XB5
CSCuk25642		12.2(2)XB4
CSCuk25721		12.2(2)XB4
CSCuk25947		12.2(2)XB4
CSCuk26562		12.2(2)XB4
CSCuk26642		12.2(2)XB4
CSCuk27924		12.2(2)XB4
CSCuk28445		12.2(2)XB4
CSCuk32311		12.2(2)XB5
CSCuk33327		12.2(2)XB5

Open Caveats—Cisco IOS Release 12.2(2)XB15

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB15 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(2)XB15.

Resolved Caveats—Cisco IOS Release 12.2(2)XB15

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB15. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx76632

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

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

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

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

- CSCea19885

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

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

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

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

- CSCea27536

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

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

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

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

- CSCea32240

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

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

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

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

- CSCea33065

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

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

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

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

- CSCea36231

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

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

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

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

- CSCea46342

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

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

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

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

- CSCea51030

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

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

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

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

- CSCea51076

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

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

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

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

- CSCea54851

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

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

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

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

- CSCeb78836

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

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

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

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

- CSCec87533

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

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

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

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

Open Caveats—Cisco IOS Release 12.2(2)XB14

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB14 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(2)XB14.

Resolved Caveats—Cisco IOS Release 12.2(2)XB14

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB14. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx76632

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

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

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

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

- CSCea19885

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

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

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

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

- CSCea27536

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

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

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

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

- CSCea32240

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

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

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

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

- CSCea33065

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

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

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

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

- CSCea36231

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

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

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

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

- CSCea46342

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

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

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

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

- CSCea51030

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

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

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

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

- CSCea51076

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

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

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

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

- CSCea54851

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

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

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

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

- CSCeb78836

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

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

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

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

Open Caveats—Cisco IOS Release 12.2(2)XB7

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB7 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(2)XB7.

Resolved Caveats—Cisco IOS Release 12.2(2)XB7

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB7. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv21918

  A router may reload if netflow-data is exported to a multicast address.

  Workaround: Do not configure a multicast address; use a unicast address instead.

- CSCdw00055

  The non-variable-length dial-plan matching character “$” permits a user to force a match on a destination-pattern consisting of a fixed number of digits.

  Workaround: Configure the destination-patterns which end in “$” to end in “T?$”:

```
!
dial-peer voice 1 voip
 destination-pattern 01152....T?$
 session target ipv4:IP_ADDR_RTR1
 ip precedence 5
!
dial-peer voice 2 voip
 destination-pattern 01152......
 session target ipv4:IP_ADDR_RTR2
 ip precedence 5
!
```

- CSCdx33166

  During LSDOCallback, the sessions on the server side go down due to which “callback already exists” debugs can be seen in the logs inhibiting callback from occurring.

  There are no known workarounds.

- CSCdx93324

  The H323 gateway may crash accessing invalid memory location.

  There are no known workarounds.

- CSCdy05296

  The port information provided on a 5400/5350/5850 on modems within Radius attribute 5 using either nas-port format a or b for async calls provide the true port information (as in slot/port) and not the TTY line number of the modem which previous generation dial platforms provided. This is causing problems for service providers using a variety of Cisco dial platforms as they are inconsistent in the information being relayed on the various platforms Cisco sells.

  There is no known workarounds.

- CSCdy14689

  In 12.2(2)XB and 12.2(4)T and later IOS codes, router does not send radius connection accounting attribute 46 for tcp clear calls or for any outbound telnet connections from router. The is issue is only with telnet connections regular ppp calls accounting records do contain this attribute just fine

  There are no known workarounds.

- CSCdy16593

  With 2930 it has been noted that some client modem (most likely a single vendor) will take the modem out of service. The error caused by this modem is not fatal to subsequent calls and should not take down the port. Under this condition the 5300 will recover but this has not been validated with all IOS releases. The 5800 does not recover.

  Modems on the AS5800 can appear to take calls even though MICA has placed them out of service. This will lower the effective CSR of the router.

  Workaround: Lower the autorecovery threshold of the modems in the configuration. This will allow the lower CSR to trigger a reset of the modems (via reload).

Open Caveats—Cisco IOS Release 12.2(2)XB6

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB6 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(2)XB6.

Resolved Caveats—Cisco IOS Release 12.2(2)XB6

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB6. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.2(2)XB6.

Open Caveats—Cisco IOS Release 12.2(2)XB5

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB5 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdx26331

  The Call History information generated by the SIP call leg does not have a valid (non-zero) duration while the POTS Call History for the same call has a non-zero duration.

  This will happen when the ACK fails to reach the TGW following an answer (200 OK response).

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(2)XB5

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB5. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdr81193

  When using MS-CHAP for inbound authentication communication with the TACACS server does not take place. The debug indicate that the TACACS was not received the traffic.

  There are no known workarounds.

- CSCds36738

  When one creates a view that contains the iso subtree, it cannot be deconfigured: a “no snmp-server view ...” command will leave the view unchanged in the running config. A reload doesn't help either.

  This has been tested on customer device (7507) running 12.0.7S1, and in our lab, on a 7513 running 12.0(8)S

  This happened all the times, even in IOS versions that have CSCdj84623 fixed. Every view can be deconfigured, except those containing the iso subtree.

  There are no known workarounds.

- CSCdu14530

  If the IP address is removed from a the PPP interface of a 7500, running 12.1E IOS, and then the IP address is added, this change is not reflected immediately in CEF. This results in 50% packet loss until the background CEF process updates the adjacency.

  Workaround: shut / no shut the PPP interface.

  Alternative workaround: Disable CEF (not an option as the 7500 is a PE router).

- CSCdv38563

  Network access server (NAS) may fail to include attributes 90 and 91 when a router hostname is used as the tunnel ID and when the tunnel ID is not included in the user profile.

  There are no known workarounds.

- CSCdv54127

  The Acct-Output-Packets and Acct-Input-Packets attributes are missing in the STOP record while testing network accounting, even though they are seen in the debug output.

  There are no known workarounds.

- CSCdv66747

  Tracebacks occur with vpdn in 12.2(02)XB, 12.2(03)PI, & 12.2.T.

  There are no known workarounds.

- CSCdv71454

  In 12.2T, “L2TP mgmt daemon” may cause CPUHOG if there are lots of packets in unsentQ.

  There are no known workarounds.

- CSCdw00924

  On a PPP multilink bundle that has multiple links, if one of the links departs from the bundle while data is enqueued for output at the bundle interface, the output mechanism on the bundle may stall, halting any further output from that bundle. The output queue on the bundle becomes full, causing packets that are forwarded to that bundle to be dropped and the affected bundle to stop transmitting packets.

  There are no known workarounds.

- CSCdw06038

  With Resource Pooling and Resource Pooling AAA accounting configured, a customer profile may not be found for a particular DNIS group.

  The access server may have a problem with incoming calls finding the customer profile depending on the order, size and value of the dnis entered; results may vary depending on whether the DNIS is manually entered or whether the wavl is set up from reload via the start-up config.

  There are no known workarounds.

- CSCdw39083

  When running test calls in a ThunderVoice environment a small percentage of the calls are being rejected by the originating gateway with cause code 47 (resource unavailable, unspecified).

  There are no known workarounds.

- CSCdw45584

  VPDN authorization fails when “lcp:send-secret=xxxx” is sent in the access accept packet from radius.

  There are no known workarounds.

- CSCdw58199

  After making an E1R2 call in a line, the consecutive attempt to bring up calls on the same line fails even with same line signalling.

  The failures are seen with all E1R2 line and register signalling combinations

  Failures seen in following images:

  c5300-js-mz-v122_2_xb_throttle.2.5.0

  c5300-js-mz.122-7.1.PI4

  c5400-js-mz.122-7.1.PI4

  c5850-p9-mz.122-7.1.PI4b

  c5300-js-mz.122-7.1.PI4a

  c5400-js-mz.122-7.1.PI4a

  c5400-js-mz.122-7.6.T.

c5400-js-mz.122-7.6.T1

c5300-js-mz.122-7.6.T.

c5300-js-mz.122-7.6.T1.

c5400-js-mz.122-7.6.PI4.Feb14

c5400-js-mz.122-7.6.PI4

c5400-js-mz-v122_2_xb_throttle.2.9.0

c5400-js-mz-v122_2_xb_throttle.2.10.0

There are no known workarounds.

- CSCdw62064

  On 7200 running 12.2.6 it is seen that with T1 links combined in a Multilink PPP bundle, and MLPPP fragmentation enabled; ISAKMP keepalives are not being received by the box, even though the remote peer is sending out the keepalive messages. As a result each end thinks its peer is dead and deletes the IKE & IPSEC SA's. They then re-negotiate IKE and IPSEC and create new SA's. As a result, IKE and IPSEC are re-negotiated at each IKE keepalive interval and there is some traffic drop during this re-negotiation phase.

  Workaround: Disable hardware crypto acceleration. With software crypto, this problem is not seen.

  Alternative workaround: Disable MLPPP fragmentation. Without fragmentation, the IKE keepalives are received by the peers (even with hardware crypto)

- CSCdw68757

  Caller on original GW of CAS hear the second dial-tone CHOM from the far end router which connected to Nortel PBX.

  This is only for CAS case.

  There are no known workarounds.

- CSCdw75532

  When using multichassis multilink, or MLP with VPDN, the box can crash.

  Workaround: Do not use MLP.

- CSCdw80521

  If an access server is configured for resource-pooling with customer profile templates, a short, abnormal call may cause the next call on that modem/interface to bind to multiple profiles causing the configuration for the next call to be different than intended.

  A workaround which works under some circumstances (but not all) is to make sure that each customer profile template explicitly specifies every configuration item which may be different on other customer profile templates to make sure the configuration items on the intended template overrides any configuration items on other templates which may be unexpectedly bound. The workaround does not work when multiple short, abnormal calls land on the same port consecutively.

- CSCdw80646

  Improper call counts on trunk groups when they are used in an SS7 environment. The trunk group may "lose" an active call when the channel is blocked from SS7 and then unblocked, while the call is still active. This would lead to the trunk group showing lesser number of calls than the actual value.

  Workaround: Wait until the calls are disconnected, at which time the call count should return to its true value, or remove the trunk from the trunk group and reconfigure it.

- CSCdw80687

  Packets are process switched on an interface with fast switching configured. This can result in high CPU usage.

  Header-compression must be configured, but only on one side. For example, in a dial-in situation, where header-compression is configured on the central switch, but not on the box that is dialling in. Also, the interface must not support FAST switched header-compression, e.g. most dial-in interfaces are currently not supported.

  Workaround: Remove header-compression from the configuration.

Note Note: If header-compression is configured on both sides of a link, and the interface does not support fast-switched header-compression, then process switching is normal and required for successful operation of the header-compression feature.

- CSCdw85178

  Genuity is not able to bill multiple customers off of one proxy.

  The are no known workarounds.

- CSCdw89455

  All PPP Auth methods will not work with MSCHAP V2.

  There are no known workarounds.

- CSCdw91279

  A Cisco router that is running Cisco IOS Release 12.2(5.7)T or a later release and that is acting as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) or L2TP network server (LNS) may fail to process valid L2TP Zero-Length Body Acknowledgement (ZLB ACK) packets. This behavior may cause sessions and tunnels to drop.

  There are no known workarounds.

- CSCdx02102

  A Cisco router may experience memory corruption when configured with software encryption (MPPE) if the MTU size is greater than 8K (and if there are actually packets of length greater than 8K).

  Workaround: Configure MTU less than 8K when doing software encryption (MPPE).

- CSCdx02525

  A Cisco access server running 12.2(3) or 12.2(4)T and later will experience a memory AAA user profiles turn on PPP header or data compression and the router is not configured to use virtual-profiles. CSCdw71698 fixes the issue for ISDN callers, however the leak continues to occur for async callers.

  Workaround: Configure virtual-profiles.

- CSCdx03583

  This problem occurs when we are interacting with MSFT's Phoenix client, and the Client send us a BYE after we've sent it a 200ok (basically, BYE and 200ok cross on the wire). In such a scenario, the MSFT client ACK's our 200ok, and leaves the call hanging (that is, it doesn't send us a BYE, as per spec). Our GW's keep the call up, till the Media Inactivity timer pops, and in effect we're hogging up the resources till then.

  Workaround: The work-around is to set a low Media Inactivity timer on the GW's and so the call resources won't be hogged up for too long. This work-around is not applicable for customers who want to set their Media Inactivity Timers to higher values.

- CSCdx05704

  When a user dials in, requests MSCB and is bound to a dialer profile, after authentication (problem won't happen if the profile is bound before PPP starts) then IOS does not propose the option to skip callback during CBCP even if we are configured for it (ppp callback accept and user has empty callback dial string).

  If the user opts to skip the callback anyway, we will drop the call because we did not propose that option, which is correct behavior but has only been enforced since CSCdu55093, which is why this bug has been relatively hidden up until recently.

  There are no known workarounds.

- CSCdx08078

  Callback fails on IOS 12.2T when configured from Radius.

  There are no known workarounds.

- CSCdx08525

  Without this fix, a regression of CSCdw23643: PPP not sending AAA Server Message in Authen Responses is inevitable.

  There are no known workarounds.

- CSCdx09410

  A CLI command in startup config is not recognized by 5800 when it boots up.

  Workaround: Manually enter that in the config after bootup.

- CSCdx11607

  AAA Pre-auth causes digital calls to break, because resource allocation fails.

  There are no known workarounds.

- CSCdx20135

  The %RADIUS-3-ALLDEADSERVER error message gets printed in the router's console even when "radius-server deadtime" is NOT configured in the global config.

  There are no known workarounds.

- CSCdx22886

  SGBP forwarding does not work if VPDN is disabled.

  Workaround: Enable VPDN (issue the **vpdn enable** command) and then disable it immediately (issue **no vpdn enable**) on all the SGBP stack group members. This allocates the resources required to do SGBP, and at the same time does not require VPDN to be kept enabled.

- CSCdx40546

  For T.37 offramp fax, the ANI information is currently available only from the message envelope of the email. But in the case that the mail has to be bounced (e.g. invalid fax machine number), the mail cannot be bounced back to the correct account. The call cannot be billed in this case.

  There are no known workarounds.

- CSCdx41547

  A voice gateway running up to version 12.2(2)XB4 configured for SIP and RADIUS will not send the “call-id” VSA to the RADIUS server when calling from telephony to SIP.

  The call-id VSA is passed correctly when calling from SIP to telephony.

  There are no known workarounds.

- CSCdx46375

  An As5400 UUT running XB throttle 4.10.0 nightly image will experience Crash at radius_build_packet() after couple of hours of stress test running Analog, ISDN, L2TP Calls.

  There are no known workarounds.

- CSCin03065

  When an attempt is made to create an additional session that has similar tunnel parameters that are defined by a RADIUS profile (for the same domain, the same user, or a different user), instead of creating a session under the existing tunnel, a new tunnel and a session are created. This condition is observed in Cisco IOS Release 12.2(7.4)T and occurs if the tunnel parameters are defined by RADIUS without either of the following definitions:

  Cisco-Avpair vpdn:tunnel-id = “xyz” or Tunnel-Client-Auth-ID = “xyz”

  Workaround: Define one of the following definitions under a RADIUS profile when tunnel parameters are defined:

  Cisco-Avpair vpdn:tunnel-id = “xyz” or Tunnel-Client-Auth-ID = “xyz”

- CSCin06313

  as5850 pops out the following error message after boot up:

  ```
  00:00:38: RM/AUTH: Process (22) failed to register to VPDN
  ```

  This message is seen with c5850-p9-mz-v122_2_xb_throttle_flo_t.0.4.0 image.

  There are no known workarounds.

- CSCuk32311

  When Cisco Express Forwarding (CEF) is enabled, adjacencies are erroneously added for sessions that have been forwarded using a tunnelling protocol such as L2TP or PPPoE. Adjacencies should only be added for sessions that terminate on the router, and only after the IP Control Protocl (IPCP) has been negotiated.

  There are no known workarounds.

- CSCuk33327

  After RADIUS failover, during EAP, the NAS would try to failover to a new RADIUS server. However, this is forbidden midway through authentication. As such, the NAS was required to restart the authentication process from scratch and allow the user another attempt to authenticate.

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.2(2)XB4

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB4 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdv38563

  Network access server (NAS) may fail to include attributes 90 and 91 when a router hostname is used as the tunnel ID and when the tunnel ID is not included in the user profile.

  There is no workaround.

- CSCdw68658

  The gateway will reject a mid-call Invite with hold sdp where the connection information (c line) is set to 0.0.0.0 and the port number of the media description (m line) is also set to 0. Instead of responding with a 200 OK response, the gateway will return a 488 Media Unacceptable response. The problem will not occur if the user agent placing the gateway on hold, sets the port number to a value other than 0.

  There is no workaround.

- CSCdw77524

  When rtp payload-type cisco-codec-fax-ind is changed from 96 to 99 then we ingress an invite with sdp rtp payload type 96 nte the gateway responds with an rtp payload type 97.

  There are no known workarounds.

- CSCin00405

  No radius accounting start or stop record is sent by the NAS when “ppp multilink” and “aaa accounting delay-start” are configured.

  Workaround is to remove one of these two commands.

Resolved Caveats—Cisco IOS Release 12.2(2)XB4

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdr47232

  Set operation is not implemented for a few dsx1 specific MIB objects like dsx1LineType, dsx1LineCoding etc.

- CSCdr85436

  Description: This command can be used in the global config mode, to enable sending radius attribute 32 (NAS-Identifier) in the accounting request. By default fully qualified domain name (FQDN) is sent in the attribute when the format is not specified.

  Syntax:

  ```
  [no] radius-server attribute 32 include-in-accounting-req {format <A string that may
  have %i, %h or %d.>}

   %i = IP address
   %h = Hostname
   %d = Domain name
  ```

  FQDN is sent by default if the format string is not configured.

  Examples:

  ```
  manly(config)#radius-server attribute 32 include-in-accounting-req format cisco %h.%d %i
  ```

  Following string will be sent in NAS-identifier as a part of accounting record.

  ```
  cisco manly.nlab.cisco.com 10.0.1.67
  ```

- CSCdr93141

  The user-maxlinks feature (see http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/maxlink.htm) does not work when configured on a VPDN LNS/HGW.

- CSCdt63321

  An IP route entry may fail to be updated properly when one-step and two-step translations are performed using the Serial Line Internet Protocol (SLIP).

  There is no workaround.

- CSCdu19432

  Attribute Acct-Session-Time [46] in Exec Acct. Stop Record is zero.

  There is no workaround.

- CSCdu35843

  IP access lists are not installed when they are received from a RADIUS server. This condition is observed in Cisco IOS Release 12.2(1.2)PI.

  There is no workaround.

- CSCdu36862

  A system accounting record needs to be sent when a radius server is added or deleted. This will be committed in latest 12.2 branch and will also be committed in latest 6400 branch.

  There are no known workarounds.

- CSCdu40402

  On AS5400, AS5800, and AS5850 access servers running Cisco IOS version 12.2XB, executing the command **show tdm mapping** will not show resource s that are used for CAS calls.

  There is no workaround.

- CSCdu40615

  Some clients may fail to successfully complete IP Control Protocol (IPCP) negotiations when thousands of PPP sessions are simultaneously reestablished, as is the case when an interface with many links is recycled. All Layer 2 Tunneling Protocol (L2TP) sessions are established, but some client virtual access interfaces may not get a negotiated IP address. The missing IP address results in lost IP connectivity on that link.

  There is no workaround.

- CSCdu64847

  CISCO-AAA-SESSION-MIB user disconnect feature doesn't work for vpdn connections on the LNS.

- CSCdu43689

  Currently, the Per-User Request buffer is limited to 600 bytes. If the user profile has more than 600 bytes of configuration information, the Per-User attributes are not processed, which results in rejecting the user.

  There is no workaround.

- CSCdu67010

  Some TACACS+ attribute string names and attribute string values have changed slightly, e.g. “nas_rx_speed” is now “nas-rx-speed”. This may cause problems for backend accounting applications trying to process records or authorization failures.

- CSCdu74728

  No accounting records are generated for outbound Telnet sessions after connection accounting is configured.

  There is no workaround.

- CSCdu84692

  When using 12.2(2.x) and 12.2(3.x)PI code, local VPDN authorization does not failover to the next method in the method list if the domain/dnis profile is not found. The workaround is to only use RADIUS/TACACS+ vpdn authorization.

- CSCdu86243

  The RADIUS attributes Ascend-Client-Primary-DNS and Ascend-Client-Secondary-DNS do not work in 12.2(3.4)T or later. The Cisco-AVPair ip:dns-server also does not work.

  There is no workaround.

- CSCdv01412

  Conditions under which the problem occurs:

```
FXS           FastEthernet           FXS(LoopBack)
 [Pots A]--------[1750_r1]--------|-------[1750_r2]

 dial-peer voice 1 voip                          dial-peer voice 2 voip
  destination-pattern 300                         destination-pattern 300
  session target ipv4:100.0.0.2                   session target loopback:rtp
```

  When A calls 300, no voice loopback occurs.

  Symptoms of the problem: silent.

  Workaround: There is no workaround.

- CSCdv01555

  Spurious access may been seen when TACACS+ is enabled in IOS versions 12.2(3.4)T or later.

  There is no workaround.

- CSCdv02732

  A router that is running Cisco IOS Release 12.2(3.4) T or a later release may reload unexpectedly after the Terminal Access Controller Access Control System (TACACS+) command accounting is enabled and a **config net** privileged EXEC command is executed. There is no workaround.

- CSCdv03076

  A Cisco router running 12.2(3.4)T or later will not process Ascend RADIUS server attributes even if “non-standard” is part of the radius-server host configuration statement if the radius-server is referenced through a aaa server group. The workaround is not to use a server-group and use group radius instead.

- CSCdv03689

  If a Point to Point Protocol (PPP) Multilink bundle interface goes down while data is flowing through it, a Cisco router may reload.

  There is no workaround.

- CSCdv04999

  The username, accounting record type, and service attributes in the command accounting record is do not have appropriate value.

  There is no workaround.

- CSCdv13634

  AAA Accounting is not done for the additional links added to Multilink PPP bundle when “aaa accounting delay-start” is configured.

  There is no workaround.

- CSCdv19031

  Currently with radius debugging turned on customers see a lot of debugs describing attributes in the packets sent and received. In order to reduce the amount of spewed out on the console a new option of 'brief' needs to be added the 'debug radius' command. This option will only indicate I/O transactions with some packet header information. Customers not turning on debugging or, not doing RADIUS wont see this problem.

- CSCdv19928

  When the Idle-Timeout attribute is received from RADIUS on an asynchronous interface, a vaccess interface is created and the timeout is not applied directly to the asynchronous interface. The Idle-Timeout attribute still works. The only side effect is that there is an extra vaccess created that is bound to the asynchronous interface.

  There is no workaround.

- CSCdv20977

  Incoming Multilink Point-to-Point Protocol (MLP) packets from an ATM interface are getting process switched when a virtual template is used for the MLP bundle configuration.

- CSCdv26709

  Certain values for Ascend-Disconnect-Cause and Ascend-Connect-Progress are recorded inaccurately in Stop messages. This is mainly observed in 122T train.

  This problem is observed with PPP sessions when using RADIUS Accounting.

  There are no workaround.

- CSCdv29468

  If a PPP client does not authenticate after agreeing to do so during LCP negotiation, the PPP session will continue to stay open in this limbo state until the client disconnects the session.

- CSCdv33270

  Under certain conditions, resources may be associated with a virtual private dialup network (VPDN) group even when there are no active calls.

  There is no workaround.

- CSCdv33313

  When network accounting is performed for PPP over ATM (PPPoA) sessions, RADIUS “start” or “stop” accounting records may occasionally fail to be sent. There is no workaround.

  Under certain conditions on a LAC, if the session is a VPDN forwarded session and the connection to the LAC is a dedicated serial line, memory can be leaked because AAA misses the stop record, so it never cleans up the AAA data for the session. This will happen if the connection continuously tries to renegotiate then attempt forwarding, which never succeeds. Eventually, the client sends a TERMREQ which restarts the session, but AAA does not get a NET STOP event so memory is leaked.

- CSCdv34768

  A Cisco router running IOS may show the following traceback when using “local-case” authentication:

  ```
  00:05:16: %AAA-3-BADMETHOD: Cannot process authentication method 2160756888
   -Process= "AAA Server", ipl= 0, pid= 26
   -Traceback= 8016F170 8016A6C8 8016AED0 8016B048 8019A94C
  ```

  There is no known workaround.

- CSCdv40116

  Reverse-access Authorization fails if the method used is Radius. Radius mandatory attribute “port” is not properly obtained causing this authorization failure.

  There is no work around.

- CSCdv40729

  In a plain bri-pri (Peer - NAS) scenario, when a call is disconnected with the command 'clear in serial0:23' on the NAS, the Ascend-Disconnect-Cause value generated is '0' (No-Reason).

  When the call is brought down by clearing the interface on the peer, it is given a value(63). If brought down by doing 'shutdown' on peer/NAS value 11 is generated. The problem occurs only with by doing clear interface on the NAS.

- CSCdv41871

  Ping fails when non-mlppp call is up on B-channel previously used to terminate mlppp call.

- CSCdv43136

  We may see some unexpected debug information during call suspend. Those debug information doesn't cause any side effect beside displaying unexpected debug information.

- CSCdv43856

  aaa attr debug does not show the tag added. This is seen in 12.2(4.2)PI. This is just a problem in debug and will not affect any other functionality.

- CSCdv54349

  When running 12.2(5.2)T and later IOS images, you may be unable to do local AAA authentication. There is no workaround. Either do AAA to a remote server or downgrade to an earlier release of code.

- CSCdv62649

  The command **ip tacacs source-interface** doesn't work properly. If configured to use loopback interface for tacacs packets, router may still use interface address.

- CSCdv64668

  The first PAP authentication after a PPP renegotiation triggered by a CONFREQ from the client will fail even though the RADIUS/TACACS+ server returns a success.

  There is no workaround.

- CSCdv67009

  The following error message may be seen on a Cisco voice gateway running the Session Initiation Protocol (SIP):

  ```
  Nov 24 20:24:12: %SIP-3-BADPAIR: Unexpected event 14 (SIPSPI_EV_CC_CALL_CONNECT) in
  state 8 (STATE_DISCONNECTING) substate 0 (SUBSTATE_NONE)
   -Traceback= 60DAD08C 60DAD7AC 6040ACD4 6040ACC0.
  ```

  This indicates that the call was cancelled while it was in the process of being brought up.

  This message can be safely ignored.

- CSCdv76649

  When the customer tries to use ^C to abort the copy operation when he prompted for confirmation, he can't break out of the copy process.

- CSCdv78693

  Spurious memory access messages appear on gatekeepers when an URQ without a call signal address in it is sent to Gateway.

  There is no work around.

- CSCdv79210

  A Cisco router gradually looses memory when Media Gateway Control Protocol (MGCP) calls are originated on the router.

  There is no workaround.

- CSCdv83040

  When using Ascend RADIUS attribute 242, IP protocols of 50 and 51 will not be accepted. This will cause users with these IPsec protocols set in their profile to be disconnected.

- CSCdv83402

  A PPPoE/PPPoA aggregation router may unexpectedly reload when many PPP events happen in a short amount of time. The router will display a STACKLOW message before reloading.

- CSCdv87754

  Symptom: A Cisco AS5850 Route Switch Controller incorrectly attempts to repeatedly netboot a Cisco IOS image if it cannot find the specified boot system image on its compact flash. The system interprets the full path of the configured boot image that failed as the image it should netboot.

  Messages similar to the following are observed:

  ```
  Sleeping for 2 secs before next netboot attempt
  %SYS-6-READ_BOOTFILE_FAIL: disk0:c5850-p9-mz File boot failed -- File not
  accessible.
  ```

  The correct behavior for a bootloader if it cannot find any specified boot images at reload time is to fall back and request the system to run the first image it can find off disk0: or bootflash:

  Conditions: Cisco AS5850 Route Switch Controllers with Cisco IOS 12.2(2)XB1 or Cisco IOS 12.2(2)XB2 bootloaders may experience this problem at reload time if the boot system image configuration points to a file on disk0: that does not exist.

  Workaround: Ensure that the boot system image configuration points to an existing and valid image on disk0:, provide additional correct boot image locations in the configuration, or use a bootloader of version Cisco IOS 12.1(5)XV3.

- CSCdw00019

  Although SGBP tunnels will still be up, SGBP bidding itself might stop working after a router has been up for sometime. This problem only occurs if two routers in the stack group receive two links of a bundle at the same time.

  Removing, and reapplying the SGBP config was sufficient to get things working again.

- CSCdw01726

  A Simple Network Management Protocol version 3 (SNMPv3) user is created using message digest 5 (MD5) authentication using the following commands:

  – **snmp group groupy v3 auth**

  – **snmp user abcdefghij groupy v3 auth md5 abcdefghij**

  An SNMP walk is performed, the configuration is saved, and the router is reloaded.

  ```
  newhope:~/src/wccp2# snmpwalk -v 3 -u abcdefghij -A abcdefghij -a MD5 -l
  AuthNoPriv 194.12.224.11
  ```

  It is working and a debug snmp header shows this:

  ```
  Incoming SNMP packet
   : v3 packet         security model: v3       security level: auth
   username: abcdefghij
  ```

A second SNMP walk is performed:

```
newhope:~/src/wccp2# snmpwalk -v 3 -u abcdefghij -A abcdefghij -a MD5 -l
 AuthNoPriv 194.12.224.11
```

After the second SNMP walk is performed, the command does not return any output and the debug snmp headers show this:

```
Incoming SNMP packet
 : v3 packet  security model: v3       security level: noauth
 : username: abcdefghij
```

There is no workaround.

- CSCdw02945

  Symptom: Incoming calls may fail to create a virtual profile even though the

  router is configured for this.

  Conditions: This problem may occur in a dial up environment where a virtual profile virtual template is defined but where no AAA authorization has been enabled This issue only occurs in 12.2 T.

  Workaround: A workaround is to configure AAA authorization e.g., **aaa authorization network default local**

- CSCdw06322

  The following error message may be seen on a Cisco voice gateway running the Session Initiation Protocol (SIP):

  ```
  Nov 24 20:24:12: %SIP-3-BADPAIR: Unexpected event 14 (SIPSPI_EV_CC_CALL_CONNECT) in
  state 8 (STATE_DISCONNECTING) substate 0 (SUBSTATE_NONE)
   -Traceback= 60DAD08C 60DAD7AC 6040ACD4 6040ACC0.
  ```

  This indicates that the call was cancelled while it was in the process of being brought up.

  This message can be safely ignored.

- CSCdw09542

  Before this fix, per-user authorization required a service type of Outbound in the Radius profile.

- CSCdw11765

  PPP Link Control Protocol (LCP) is not accepting sent CONFACK negotiated on a asynchronous interface for a virtual profile.

  There is no workaround.

- CSCdw13432

  When the called party is busy in a two-stage call scenario, the calling party may not hear a busy tone and the call terminates immediately. This behavior is observed with Cisco IOS Release 12.2(2)XB, Release 12.2(7), and some earlier 12.2 releases.

  There is no workaround.

- CSCdw18785

  When a 302 redirect is received after a 18x with a COntact header the outgoing INVITE will have the request uri of the Contact in the 18x. It should use the Contact of the 302.

  Workaround: Disabling rel1xx on the router.

- CSCdw23836

  When a 18x is received which was sent reliably, a PRACK needs to be sent. Subsequent 18x's received that match the previous one's call leg do not receive a PRACK. A workaround is to disable reliable provisional responses.

- CSCdw25746

  Symptom: Cisco Voice Gateways may experience a reload especially when running high levels of traffic.

  Conditions: This problem may be experienced in 12.2(2)XB2 and 12.2 mainline releases.

  Workaround: none

- CSCdw28786

  When the customer tries to use ^C to abort the copy operation when he prompted for confirmation, he can't break out of the copy process.

- CSCdw30994

  When downloading IP pools from a AAA server, there is no way to define a non-contiguous range of addresses using multiple statements like this:

  ```
  "ip:pool-def#1=aol-pool 192.168.232.0 192.168.237.255",
   "ip:pool-def#2=aol-pool 192.168.238.1 192.168.238.160"
  ```

  When those statements are applied, the second pool-def overwrites the first one. Defining the pools on the command line yields the expected result. This only happens in 12.2(2)XB ED release train. 12.1/12.2 does not exhibit this behavior.

- CSCdw35046

  A Cisco router may reload when proxied RADIUS is used for authentication and accounting.

  There is no workaround.

- CSCdw35930

  The command **aaa authentication attempts login <n>** appears in the configuration if the command **tacacs-server attempts <n>** is present in the configuration. Changes to either command will be reflected in the other. Also, the number of attempts granted is actually one less than the number configured. The workaround is to configure one more attempt than the number you actually want.

- CSCdw43862

  For some devices that are not conforming to V.110 async to sync padding requirements, this **cli** command allow the users to disable the padding.

- CSCdw46065

  A Cisco router that is used as a gateway may reload if one of multiple record routes that are received on the gateway is invalid.

  There is no workaround.

- CSCdw53071

  If a second call is made after the first call is completely disconnected (by hanging up the phone instead of using the flash feature to switch between two calls), the second call may fail.

  There is no workaround.

- CSCdw53243

  In a Cisco Signaling System 7 (SS7) Interconnect for Voice Gateways solution, if a Cisco AS5400 universal access gateway receives an incoming time-division multiplexing (TDM) call (NI-2, PRI, channel-associated signaling [CAS]) with a called number that does not match a configured dial-peer, the call will be connected to a modem, and a modem tone will be played back to the calling party. This is normal behavior, however there is no configurable option for such to be rejected instead of being treated as a modem call.

- CSCdw62969

  A network access server (NAS) that is running Cisco IOS Release 12.2(02)XB3 or Release 12.2(8)T may reload when Layer 2 forwarding (L2F) virtual private dial-up network (VPDN) calls are placed using an authentication, authorization, and accounting (AAA) VPDN user profile that does not contain the RADIUS class (25) attribute.

  Workaround: Configure a dummy RADIUS class (25) attribute in the VPDN user profile on the AAA server.

- CSCdw66251

  SIP gateway midcall INVITE requests in the called to calling party direction will have the Route header constructed incorrectly. ACK requests in the called to calling party direction will have the request URI constructed incorrectly. This could cause some operations such as T.38 fax relay to fail.

  This problem can occur only if two or more SIP proxies are in the SIP signalling path and the Record Route feature is enabled.

  There is no workaround.

- CSCuk25642

  When using callin authentication on a LSDO call with RADIUS, PPP sends multiple authorization requests to AAA. This will slow down call setup but have no functional impact.

- CSCuk25721

  RADIUS CLID attribute was missing for large scale dialout accounting.

- CSCuk25947

  If PPP authentication is configured on an interface and if a user negotiates a callback during a Link Control Protocol (LCP) operation, the call will fail if the user does not have any callback information configured.

  There is no workaround.

- CSCuk26562

  AAA id debugging was not clear and displayed far too much information.

- CSCuk26642

  RADIUS calls with a non-RFC supported value were accepted when they should be rejected.

- CSCuk27924

  send-auth would not be applied on the NAS, but rather the value of auth-type would be used instead.

- CSCuk28445

  We now store a generic 'wrapper' record which holds information in the tree, generic to all accounting records. This way, we are not impacted by the life-span of any one accounting record.

Open Caveats—Cisco IOS Release 12.2(2)XB3

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB3 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(2)XB3.

Resolved Caveats—Cisco IOS Release 12.2(2)XB3

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw65903

  An error can occur with management protocol processing. Please use the following URL for further information:

  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats—Cisco IOS Release 12.2(2)XB2

This section documents possible unexpected behavior by Cisco IOS Release 12.2(2)XB 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(2)XB2.

Resolved Caveats—Cisco IOS Release 12.2(2)XB2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(2)XB2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

There are no known resolved caveats for Cisco IOS Release 12.2(2)XB2.

Open Caveats—Cisco IOS Release 12.2(2)XB

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

- CSCdt55987

  A Cisco 7200 series router may have some active calls dropped if a Haydn+ card performs Online Insertion and Removal (OIR) while active calls are present.

  Workaround: Do not perform an OIR when active calls are present.

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 37
- Platform-Specific Documents, page 38
- Feature Modules, page 38
- Cisco IOS Software Documentation Set, page 39

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(2)XB*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2 XB" 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(2)XB 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 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. 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 5 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• Cisco IOS Configuration Fundamentals Configuration Guide • Cisco IOS Configuration Fundamentals Command Reference	Cisco IOS User Interfaces File Management System Management
• Cisco IOS Bridging and IBM Networking Configuration Guide • Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2 • Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• Cisco IOS Dial Technologies Configuration Guide: Dial Access • Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications • Cisco IOS Dial Technologies Command Reference, Volume 1 of 2 • Cisco IOS Dial Technologies Command Reference, Volume 2 of 2	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• Cisco IOS IP Configuration Guide • Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services • Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols • Cisco IOS IP Command Reference, Volume 3 of 3: Multicast	IP Addressing IP Services IP Routing Protocols IP Multicast
• Cisco IOS AppleTalk and Novell IPX Configuration Guide • Cisco IOS AppleTalk and Novell IPX Command Reference	AppleTalk Novell IPX
• Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide • Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• Cisco IOS Voice, Video, and Fax Configuration Guide • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• Cisco IOS Quality of Service Solutions Configuration Guide • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• Cisco IOS Security Configuration Guide • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• Cisco IOS Switching Services Configuration Guide • Cisco IOS Switching Services Command Reference	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• Cisco IOS Wide-Area Networking Configuration Guide • Cisco IOS Wide-Area Networking Command *Reference*	ATM Frame Relay SMDS X.25 and LAPB
• Cisco IOS Mobile Wireless Configuration Guide • Cisco IOS Mobile Wireless Command Reference	General Packet Radio Service
• Cisco IOS Terminal Services Configuration Guide • Cisco IOS Terminal Services Command Reference	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • Cisco IOS Debug Command Reference • Cisco IOS Software System Error Messages • *New Features in 12.2-Based Limited Lifetime Releases* • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

The following sections 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 37.