



Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(8)YL

August 1, 2003

These release notes describe new features and significant software components for the Cisco 1700 series routers that support Cisco IOS Release 12.2 T, up to and including Release 12.2(8)YL1. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the [Cross-Platform Release Notes for Cisco IOS Release 12.2 T](#) located on CCO and the Documentation CD.

For a list of the software caveats that apply to Release 12.2(8)YL1, refer to the section “**Caveats**” and to the online [Caveats for Cisco IOS Release 12.2 T](#) document. The caveats document is updated for every 12.2 T maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD.

Contents

These release notes discuss the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 8](#)
- [Limitations, page 10](#)
- [Important Notes, page 11](#)
- [Caveats, page 12](#)
- [Related Documentation, page 15](#)
- [Obtaining Documentation, page 16](#)
- [Obtaining Technical Assistance, page 17](#)



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

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

System Requirements

This section describes the system requirements for Release 12.2(8)YL1 and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 4](#)
- [Determining the Software Version, page 4](#)
- [Upgrading to a New Software Release, page 5](#)
- [Feature Set Tables, page 5](#)

Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Release 12.2(8)YL1 on the Cisco 1700 series routers.

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1710 Routers	Cisco 1710 IOS IP Plus IPX/AT/IBM/ FW/IDS IPSec 3DES	IP Plus IPX/AT/IBM/ FW/IDS IPSec 3DES	c1710-bk9no3r2sy-mz	16 MB	48 MB
	Cisco 1710 IOS IP Plus FW/IDS IPSec 3DES	IP Plus FW/IDS IPSec 3DES	c1710-k9o3sy-mz	8 MB	48 MB
Cisco 1720, Cisco 1721, Cisco 1750, Cisco 1751, and Cisco 1760	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM/FW/IDS IPSec 3DES	IP Plus ADSL/IPX/ AT/IBM/FW/IDS IPSec 3DES	c1700-bk9no3r2sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM	IP Plus ADSL/IPX/ AT/IBM	c1700-bnr2sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/IPX/AT/IBM	IP/IPX/AT/IBM	c1700-bnr2y-mz	8 MB	32 MB
	Cisco 1700 IOS IP Plus ADSL/FW/IDS IPSec 56	IP Plus ADSL/FW/IDS IPSec 56	c1700-k8o3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL IPSec 56	IP Plus ADSL IPSec 56	c1700-k8sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL/FW/ IDS IPSec 3DES	IP Plus ADSL/FW/ IDS IPSec 3DES	c1700-k9o3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL IPSec 3DES	IP Plus ADSL IPSec 3DES	c1700-k9sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ FW/IDS	IP Plus ADSL/IPX/ FW/IDS	c1700-no3sy7-mz	16 MB	48 MB
	Cisco 1700 IOS IP/IPX	IP/IPX	c1700-ny-mz	8 MB	32 MB
	Cisco 1700 IOS IP/FW/IDS	IP/FW/IDS	c1700-o3y-mz	8 MB	32 MB
	Cisco 1700 IOS IP Plus	IP Plus	c1700-sy-mz	16 MB	32 MB
	Cisco 1700 IOS IP Plus ADSL	IP Plus ADSL	c1700-sy7-mz	16 MB	48 MB
Cisco 1700 IOS IP	IP	c1700-y-mz	8 MB	32 MB	

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
	Cisco 1700 IOS IP/ADSL	IP/ADSL	c1700-y7-mz	8 MB	32 MB
Cisco 1721, Cisco 1751, and Cisco 1760	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM/FW/IDS IPSec 56	IP Plus ADSL/IPX/ AT/IBM/FW/IDS IPSec 56	c1700-bk8no3r2sy7-mz	16 MB	64 MB
Cisco 1750, Cisco 1751, and Cisco 1760	Cisco 1700 IOS IP Plus Voice	IP Plus Voice	c1700-sv3y-mz	16 MB	48 MB
Cisco 1751 and Cisco 1760	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM/Voice/FW/IDS IPSec 56	IP Plus ADSL/IPX/ AT/IBM/Voice/FW/ IDS IPSec 56	c1700-bk8no3r2sv3y7-mz	32 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM/VOX/FW/IDS IPSec 56	IP Plus ADSL/IPX/ AT/IBM/VOX/FW/ IDS IPSec 56	c1700-bk8no3r2sv8y7-mz	32 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM/Voice/FW/IDS IPSec 3DES	IP Plus ADSL/IPX/ AT/IBM/Voice/FW/ IDS IPSec 3DES	c1700-bk9no3r2sv3y7-mz	32 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ AT/IBM/VOX/FW/IDS IPSec 3DES	IP Plus ADSL/IPX/ AT/IBM/VOX/FW/ IDS IPSec 3DES	c1700-bk9no3r2sv8y7-mz	32 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice/ FW/IDS IPSec 56	IP Plus ADSL/Voice/ FW/IDS IPSec 56	c1700-k8o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX/ FW/IDS IPSec 56	IP Plus ADSL/VOX/ FW/IDS IPSec 56	c1700-k8o3sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice IPSec 56	IP Plus ADSL/Voice IPSec 56	c1700-k8sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX IPSec 56	IP Plus ADSL/VOX IPSec 56	c1700-k8sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice/ FW/IDS IPSec 3DES	IP Plus ADSL/Voice/ FW/IDS IPSec 3DES	c1700-k9o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX/ FW/IDS IPSec 3DES	IP Plus ADSL/VOX/ FW/IDS IPSec 3DES	c1700-k9o3sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice IPSec 3DES	IP Plus ADSL/Voice IPSec 3DES	c1700-k9sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX IPSec 3DES	IP Plus ADSL/VOX IPSec 3DES	c1700-k9sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ Voice/FW/IDS	IP Plus ADSL/IPX/ Voice/FW/IDS	c1700-no3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/IPX/ VOX/FW/IDS	IP Plus ADSL/IPX/ VOX/FW/IDS	c1700-no3sv8y7-mz	16 MB	64 MB

Table 1 Recommended Memory for the Cisco 1700 Series Routers

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM Memory
Cisco 1751 and Cisco 1760 (Continued)	Cisco 1700 IOS IP Plus ADSL/Voice/ FW/IDS	IP Plus ADSL/Voice/ FW/IDS	c1700-o3sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX/ FW/IDS	IP Plus ADSL/VOX/ FW/IDS	c1700-o3sv8y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/Voice	IP Plus ADSL/Voice	c1700-sv3y7-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus VOX	IP Plus VOX	c1700-sv8y-mz	16 MB	64 MB
	Cisco 1700 IOS IP Plus ADSL/VOX	IP Plus ADSL/VOX	c1700-sv8y7-mz	16 MB	64 MB

Hardware Supported

Cisco IOS Release 12.2(8)YL1 supports the following Cisco 1700 series routers:

- Cisco 1710 Routers
- Cisco 1720 Routers
- Cisco 1721 Router
- Cisco 1750, 1750-2V, and 1750-4V Routers
- Cisco 1751 and 1751-V Routers
- Cisco 1760 and 1760-V Routers

The Cisco 1710, 1720, and 1721 routers run data images only. The Cisco 1750, 1750-2V, and 1750-4V routers run data or data-and-voice images, providing analog voice support. Cisco 1751, 1751-V, 1760, and 1760-V routers run data or data-and-voice images, providing digital and analog voice support.

For detailed descriptions of new hardware features and which features are supported on each router, see the “[New and Changed Information](#)” section on page 8. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to Cisco 1700 series routers, which are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:

[Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1700 Series Routers: <platform_name>](#)

Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 1700 series router, log in to the router and enter the **show version EXEC** command. The following sample output from the **show version** command indicates the version number on the second output line:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-Y-MZ), Version 12.2(8)YL1, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)
Synched to technology version 12.2(5.4)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see *Software Installation and Upgrade Procedures* located at: http://www.cisco.com/warp/public/130/upgrade_index.shtml.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.2(8)YL1 supports the same feature sets as Releases 12.2 and 12.2(8)T, but Release 12.2(8)YL1 includes new features supported by the Cisco 1700 series routers.



Caution

Cisco IOS images with strong encryption (including, but not limited to 168-bit (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 can be denied or subject to delay due to United States government regulations. When applicable, the purchaser/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 through Table 6 list the features and feature sets supported in Cisco IOS Release 12.2(8)YL1:

- Table 2—Cisco 1710 routers
- Table 3—Cisco 1720, 1721, 1750, 1751, and 1760 routers
- Table 4—Cisco 1721, 1751, and 1760 routers
- Table 5—Cisco 1750, 1751, and 1760 routers
- Table 6—Cisco 1751 and 1760 routers

The tables use 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, “12.2(8)YL” means the feature was introduced in 12.2(8)YL. If a cell in this column is empty, the feature was included in a previous release or the initial base release.



Note

These feature set tables only contain a selected list of features, which are cumulative for Release 12.2(8)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* and Release 12.2 T Cisco IOS documentation.

Table 2 Feature List by Feature Set for Cisco 1710 Routers

Feature	In	Feature Set	
		IP/IPX/AT/IBM/ FW/IDS Plus IPSec 3DES	IP Plus FW/IDS IPSec 3DES
Security			
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	Yes	Yes
Voice			
Voice Support on Digital T1/E1 Interfaces		No	No

Table 3 Feature List by Feature Set for Cisco 1720, 1721, 1750, 1751, and 1760 Routers, Part 1 of 2

Feature	In	Feature Set						
		IP Plus ADSL/ IPX/AT/IBM/ FW/IDS IPSec 3DES	IP Plus ADSL/IPX/ AT/IBM	IP/IPX/AT/ IBM	IP Plus ADSL/FW/ IDS IPSec 56	IP Plus ADSL IPSec 56	IP Plus ADSL/FW/ IDS IPSec 3DES	IP Plus ADSL IPSec 3DES
Security								
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	Yes	No	No	Yes	Yes	Yes	Yes
Voice								
Voice Support on Digital T1/E1 Interfaces		No	No	No	No	No	No	No

Table 3 Feature List by Feature Set for Cisco 1720, 1721, 1750, 1751, and 1760 Routers, Part 2 of 2

Feature	In	Feature Set						
		IP Plus ADSL/ IPX/ FW/IDS	IP/IPX	IP/FW/IDS	IP Plus	IP Plus ADSL	IP	IP/ ADSL
Security								
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	No	No	No	No	No	No	No
Voice								
Voice Support on Digital T1/E1 Interfaces		No	No	No	No	No	No	No

Table 4 Feature List by Feature Set for Cisco 1721, 1751, and 1760 Routers

Feature	In	Feature Set
		IP Plus ADSL/IPX/ AT/IBM/FW/IDS IPSec 56
Security		
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	Yes
Voice		
Voice Support on Digital T1/E1 Interfaces		No

Table 5 Feature List by Feature Set for Cisco 1750, 1751, and 1760 Routers

Feature	In	Feature Set
		IP Plus Voice
Security		
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	No
Voice		
Voice Support on Digital T1/E1 Interfaces		No

Table 6 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 1 of 3

Feature	In	Feature Set					
		IP Plus ADSL/IPX/ AT/IBM/ Voice/FW/ IDS IPSec 56	IP Plus ADSL/ IPX/ AT/IBM/ VOX/FW/IDS IPSec 56	IP Plus ADSL/ IPX/ AT/IBM/ Voice/FW/IDS IPSec 3DES	IP Plus ADSL/ IPX/ AT/IBM/ VOX/FW/IDS IPSec 3DES	IP Plus ADSL/Voice/ FW/IDS IPSec 56	IP Plus ADSL/VOX/ FW/IDS IPSec 56
Security							
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	Yes	Yes	Yes	Yes	Yes	Yes
Voice							
Voice Support on Digital T1/E1 Interfaces		No	Yes	No	Yes	No	Yes

Table 6 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 2 of 3

Feature	In	Feature Set					
		IP Plus ADSL/Voice IPSec 56	IP Plus ADSL/VOX IPSec 56	IP Plus ADSL/Voice / FW/IDS IPSec 3DES	IP Plus ADSL/VOX/ FW/IDS IPSec 3DES	IP Plus ADSL/Voice IPSec 3DES	IP Plus ADSL/VOX/ IPSec 3DES
Security							
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	Yes	Yes	Yes	Yes	Yes	Yes
Voice							
Voice Support on Digital T1/E1 Interfaces		No	Yes	No	Yes	No	Yes

Table 6 Feature List by Feature Set for Cisco 1751 and 1760 Routers, Part 3 of 3

Feature	In	Feature Set						
		IP Plus ADSL/IPX/ Voice/FW/ IDS	IP Plus ADSL/IPX/ VOX/FW/IDS	IP Plus ADSL/ Voice/ FW/IDS	IP Plus ADSL/VOX/ FW/IDS	IP Plus ADSL/ Voice	IP Plus VOX	IP Plus ADSL/ VOX
Security								
Software Based LZ Compression with Hardware Encryption	12.2(8)YL	No	No	No	No	No	No	No
Voice								
Voice Support on Digital T1/E1 Interfaces		No	Yes	No	Yes	No	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 1700 series routers for Release 12.2.(8)YL.

New Software Features in Release 12.2(8)YL

The following sections describe the new software features supported by the Cisco 1700 series routers for Release 12.2.(8)YL.

Software Based LZ Compression with Hardware Encryption

This feature enables the Cisco 1700 Series routers to support Layer 3 compression (through use of the Lempel-Ziv, or LZ, standard) in software with hardware-based IPSec encryption. Previously, this combination could not be supported.

Benefits

One benefit of this feature is that, through LZ compression, encrypted packets being transmitted are decreased in size, resulting in reduced WAN bandwidth demands. This allows VPNs to be supported more effectively in regions of the world that only utilize low-speed WAN links.

Additionally, by supporting LZ compression with hardware encryption, greater processing power is used for the encryption process, thereby increasing performance. By combining LZ compression with hardware encryption, customers can realize high performance VPNs with reduced bandwidth demands.

Voice Support on Digital T1/E1 Interfaces

Release 12.2(8)YL1 adds voice support to digital T1/E1 interfaces. All the voice functionality that has been supported on analog interfaces (Release 12.2(4)YB) will now be supported on digital T1/E1 interfaces.

The features that are included in this voice support are the following:

- MGCP VoIP call admission control
- MGCP-based fax (T.38) and DTMF relay
- Interactive Voice Response (IVR), Version 2.0
- MGCP 1.0
- Hoot and Holler over IP
- Call admission control for H.323 VoIP gateways
- T.37 store and forward fax
- Session Initiation Protocol (SIP) for VoIP enhancements
- ISDN progress indicator support for SIP using 183 Session Progress
- SIP intra-gateway hairpinning
- SIP diversion header implementation for redirecting number
- SIP configurable PSTN cause code mapping
- SIP T.38 fax relay
- SIP call transfer using refer method
- SIP gateway support for bind command
- SIP gateway support for third party call control
- DTMF relay for SIP calls using named telephone events
- SIP gateway support of RSVP
- Cisco IOS Telephony Service Version 2.0, and Survivable Remote Site Telephony (SRSTelephony)
- VoFR, H.323 Version 2 support

See the following Cisco IOS release notes for further information regarding these features:

- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(4\)YB](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(4\)XM](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(4\)XW](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(2\)XT](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(2\)XH](#)

New Software Features in Release 12.2(8)T

For information regarding the features supported in Cisco IOS Release 12.2 T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on CCO:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/xprn122t/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.2T)

Limitations

Data Compression

Packets of size less than 128 bytes or greater than 5000 bytes will not be compressed. Also, all cases of degenerative compression, where the packet is actually expanded rather than compressed, will be discarded, and the original packets will be forwarded.

Maximum Number of Store and Forward Fax Calls

The Cisco 1751 router supports 30 voice calls and the Cisco 1760 router supports 48 voice calls. However, these routers might not be able support more than 10 store and forward fax calls due to memory constraints.

Additional Restriction Information

See the following Cisco IOS release notes for further information regarding limitations and restrictions:

- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(8\)YJ](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(4\)YB](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(4\)XM](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(4\)XW](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(2\)XT](#)
- [Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2\(2\)XH](#)

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2.(8)YL that can apply to the Cisco 1700 series routers. (Also, see the [“Caveats” section on page 12.](#))

T1/E1 VWIC Support on Cisco 1751 and 1760 Routers

The Cisco 1751 and 1760 routers no longer need a voice image to support data applications on T1/E1 VWICs.

Fan Operation in Cisco 1700 Series Routers

Cisco 1760 and 1760-V router fans are always on, and Cisco 1710 routers do not contain a fan. However, the fans in Cisco 1720, 1721, 1750, and 1751 routers stay off until thermally activated.

Flash defaults to Flash:1 on Multipartition Flash

When using a multipartition flash card, the various flash partitions are referred to as “flash:1:”, “flash:2:”, etc. If you specify only “flash” in a multipartition flash, the parser assumes “flash:1:.” For example, if you enter **show flash all** the parser defaults to “show flash:1: all” and only the flash information for the first partition displays. To see information for all flash partitions, enter **show flash ?**. This will list all of the valid partitions. Then enter **show flash:xx: all** on each valid partition.

Peak Cell Rate and Sustainable Cell Rate Values

On Cisco 1700 routers, specify the Peak Cell Rate (PCR) and Sustainable Cell Rate (SCR) as multiples of 32 Kbps. Other rates are treated as the next lower value of a multiple of 32. For example, an entered PCR value of 150 is considered 128.

Using the boot flash Command

Booting a Cisco 1700 series router with the commands **boot flash** or **boot system flash** results in unpredictable behavior. To work around this problem, be sure to enter a colon (:) following both commands (for example, **boot flash:** or **boot system flash:**).

Using Dialer Interface with MLPPPoATM

This feature is not supported on the Cisco 1700 series platforms. Please use the Virtual Template interface instead.

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Release 12.2 T are also in Release 12.2(8)YL1. For information on caveats in Cisco IOS Release 12.2 T, refer to the [Caveats for Cisco IOS Release 12.2 T](#) document. For information on caveats in Cisco IOS Release 12.2, refer to the [Caveats for Cisco IOS Release 12.2](#) document. These documents list severity 1 and 2 caveats, and are located on CCO and the Documentation CD.

**Note**

If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats - Release 12.2(8)YL1

Cisco IOS Release 12.2(8)YL1 is a rebuild release for Cisco IOS Release 12.2(8)YL. This section describes unexpected behavior that is fixed in Release 12.2(8)YL1.

Miscellaneous

CSCdz71127

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

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

This advisory is available at

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

CSCea02355

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

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

This advisory is available at

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

Open Caveats - Release 12.2(8)YL

This section describes unexpected behavior in Release 12.2.(8)YL.

Miscellaneous

CSCdx19900

Packet greater than 5000 bytes fails when SW compression with HW encryption is done.

CSCdx32291

Crypto console error generated when tunnel is initiated via EM module.

CSCdx63850

Broadcast address is being sent as MAC Address in the Cisco 1720, 1721 and 1750 routers when an Ethernet WIC is in slot 1. When there is a one-port Ethernet WIC (WIC-1E) in slot 1 and a TLV 4 EEPROM WIC, like an ADSL WIC, in slot 0, the MAC Address of the Ethernet interface is incorrectly set to the broadcast address ffff.ffff.ffff. The work-around for this problem is to place the Ethernet WIC in slot 0 only.

CSCdx64971

IPSec does not work when **set pfs group#** is in the configuration. For example:

```
crypto ap mymap1 11 ipsec-isakmp
  set peer 10.0.0.1
  set security-association level per-host
  set transform-set 1+5+8
  set pfs group2
  match address 101
```

The work-around for this problem is to remove **set pfs group#** from the configuration.

CSCdx90637

A Cisco 1700 Series router with a WIC-2AM (2-port asynchronous interface) may reload while issuing the **ipx routing** CLI. The work-around is to configure ipx routing without running traffic.

CSCdy03960

When configuring MLP, the Cisco 1720 router CPEs crash when an interface is entered into a multilink group. No work-around is available, but it is known that the problem will not occur when using images from Cisco IOS Release 12.2(4)XL.

CSCdy05964

The Cisco 1760 router crashes at bootup if both VIC-2FXO-EU and VIC-2FXO-M3 interface cards are inserted. Additionally, having the VIC-2FXO-EU card inserted alone will cause a traceback at bootup. There is no work-around.

CSCdy07777

A traceback appears on the router when MGCP calls are made with RSVP, causing the call to fail. This happens when using Call Admission Control with RSVP for MGCP calls. A work-around for this problem is to create a dummy dial-peer as follows:

```
dial-peer voice 1000 voip
req-qos guaranteed-delay
```

CSCin10786

Crash observed when T1 card is in slot 0 and **rqnt** is sent.

CSCin11036

IVR application is not played in MGCP when sent through CRCX.

CSCin11039

GW uses Cisco fax-relay mode if **fx=gw** is used in LCO.

Resolved Caveats - Release 12.2(8)YL

This section describes unexpected behavior that is fixed in Release 12.2(8)YL.

Miscellaneous

CSCin09241

The “IPV4_ADDR” identity only is supported.

CSCdw25878

When using SIP, the URL name in the terminating message is not the same as the URL name in the originating message. An IP address shows up instead.

CSCdw92918

Using “bvi/irb/network-extension mode”, unable to ping server.

CSCdx47760

If an IP Address is acquired through DHCP and the interface is subsequently shut down, the IP address is not assigned to the Fast Ethernet interface after you enter the following command for the interface: **ip address a.b.c.d mask**. This occurs on all 1700 platforms.

CSCdy03472

Cisco 1700 Series router with ADSL WIC fails to boot due to insufficient memory.

CSCdy13841

After “service-policy output x” is configured on CE's outbound interface to PE, multi-vrf can only ping the first VRF and the pings to remaining VRFs will fail. Problem remains even after “service-policy output x” is removed.

Related Documentation

The following sections describe the documentation available for the Cisco 1700 series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration 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.

Use these release notes with the documents listed in the following sections:

- [Release-Specific Documents](#)
- [Platform-Specific Documents](#)

Release-Specific Documents

The following documents are specific to Release 12.2 and apply to Release 12.2(8)YL1. They are located on Cisco.com and the Documentation CD (under the heading **Service & Support**):

- To reach the *Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.2(8)YJ*, click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cisco 1700 Series Routers: Cisco 1700 Series - Release Notes for Release 12.2(8)YJ
- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.2 T*, click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Release Notes: Cisco IOS Release 12.2 T
- To reach product bulletins, field notices, and other release-specific documents, click this path:
Technical Documents: Product Bulletins
- To reach the *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2, click this path:
Technical Documents: Cisco IOS Software: Release 12.2: Caveats


Note

If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to Cisco 1700 series routers are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1700/index.htm

This URL is subject to change without notice. If it changes, point your web browser to CCO, and click the following path:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 1700 Series Routers: <platform_name>

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at this URL:

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

Documentation CD-ROM

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

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

<http://www.cisco.com/tac>

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

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

