



Release Notes for Cisco 1700 Series Routers for Cisco IOS Release 12.3(4)XG5

August 08, 2007
OL-5487-07

These release notes describe new features and significant software components for Cisco 1700 series routers that support Cisco IOS Release 12.3(4)T, up to and including Cisco IOS Release 12.3(4)XG5. 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 12.3T](#) located on [Cisco.com](#).

For a list of the software caveats that apply to Cisco IOS Release 12.3(4)XG5, see the “[Caveats](#)” section on [page 9](#) and [Caveats for Cisco IOS Release 12.3\(4\)T](#). The online caveats document is updated for every maintenance release and is located on [Cisco.com](#).

Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 7](#)
- [Limitations and Restrictions, page 8](#)
- [Caveats, page 9](#)
- [Related Documentation, page 21](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 26](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes system requirements for Cisco IOS Cisco IOS Release 12.3(4)XG5 and includes the following sections:

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

Memory Requirements

[Table 1](#) describes memory requirements for legacy images and [Table 2](#) describes memory requirements for cross-platform images for Cisco IOS feature sets supported by Cisco IOS Cisco IOS Release 12.3(4)XG5 on Cisco 1700 series routers.

Table 1 Recommended Memory for Cisco 1700 Series Routers—Legacy Images

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1710	Cisco 1710 IOS IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES	IP/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES	c1710-bk9no3r2sy-mz	16 MB	96 MB
	Cisco 1710 IOS IP/FW/IDS PLUS IPSEC 3DES	IP/FW/IDS PLUS IPSEC 3DES	c1710-k9o3sy-mz	16 MB	64 MB
Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP/ADSL/VOX PLUS	IP/ADSL/VOX PLUS	c1700-sv8y7-mz	32 MB	96 MB
	Cisco 1700 IOS IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	IP/ADSL/VOX/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sv8y7-mz	32 MB	96 MB
	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/VOX/FW/IDS PLUS IPSEC 3DES	IP/ADSL/IPX/AT/IBM/VOX/FW/IDS PLUS IPSEC 3DES	c1700-bk9no3r2sv8y7-mz	32 MB	128 MB
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP/ADSL PLUS	IP/ADSL PLUS	c1700-sy7-mz	16 MB	64 MB
Cisco 1720, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP	IP	c1700-y-mz	16 MB	48 MB

Table 1 Recommended Memory for Cisco 1700 Series Routers—Legacy Images (continued)

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP/ADSL/IPX/AT/ IBM PLUS	IP/ADSL/IPX/AT/ IBM PLUS	c1700-bnr2sy7-mz	16 MB	96 MB
Cisco 1701, Cisco 1711, Cisco 1712, Cisco 1721, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP/ADSL/IPX/AT/ IBM/FW/IDS PLUS IPSEC 3DES	IP/ADSL/IPX/AT/ IBM/FW/IDS PLUS IPSEC 3DES	c1700-bk9no3r2sy7-mz	32 MB	96 MB
Cisco 1701, Cisco 1720, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP/ADSL	IP/ADSL	c1700-y7-mz	16 MB	48 MB
Cisco 1701, Cisco 1711, Cisco 1712, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES	IP/ADSL/FW/IDS PLUS IPSEC 3DES	c1700-k9o3sy7-mz	16 MB	64 MB

Table 2 Recommended Memory for Cisco 1700 Series Routers—Cross-Platform Images

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP BASE	IP BASE	c1700-ipbase-mz	16 MB	64 MB
Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS IP VOICE	IP VOICE	c1700-ipvoice-mz	32 MB	96 MB
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS ENTERPRISE BASE	ENTERPRISE BASE	c1700-entbase-mz	16 MB	64 MB

Table 2 Recommended Memory for Cisco 1700 Series Routers—Cross-Platform Images (continued)

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1701, Cisco 1711, Cisco 1712, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS ADVANCED SECURITY	ADVANCED SECURITY	c1700-advsecurityk9-mz	16 MB	64 MB
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS SP SERVICES	SP SERVICES	c1700-spservicesk9-mz	32 MB	96 MB
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS ENTERPRISE SERVICES	ENTERPRISE SERVICES	c1700-entservicesk9-mz	32 MB	96 MB
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS ADVANCED IP SERVICES	ADVANCED IP SERVICES	c1700-advipservicesk9-mz	32 MB	96 MB
Cisco 1701, Cisco 1711, Cisco 1712, Cisco 1721, Cisco 1751, Cisco 1751-V, Cisco 1760	Cisco 1700 IOS ADVANCED ENTERPRISE SERVICES	ADVANCED ENTERPRISE SERVICES	c1700-adventerprisek9-mz	32 MB	128 MB

Hardware Supported

Cisco IOS Cisco IOS Release 12.3(4)XG5 supports the following Cisco 1700 series routers:

- Cisco 1701
- Cisco 1710
- Cisco 1711
- Cisco 1712
- Cisco 1720

- Cisco 1721
- Cisco 1751 and 1751-V
- Cisco 1760

Cisco 1701, Cisco 1710, Cisco 1711, Cisco 1712, Cisco 1720, and Cisco 1721 routers run data images only. Cisco 1751, Cisco 1751-V, and Cisco 1760 routers run data or data-and-voice images, providing digital and analog voice support.

Cisco 1711 and Cisco 1712 routers run the following IPsec Triple Data Encryption Standard (3DES) images only:

- Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES
- Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES
- Cisco 1700 Advanced Security
- Cisco 1700 IOS ADVANCED ENTERPRISE SERVICES

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](http://www.cisco.com) 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 [Cisco.com](http://www.cisco.com), and follow this path:

Technical Documentation > Routers > Modular Access Routers > Cisco 1700 Series Routers > <platform name>

Determining the Software Version

To determine which version of Cisco IOS software is 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.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-Y7-MZ), Version 12.4(11)XJ5, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.3(5.7)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see [Cisco IOS Software Releases 12.3 T Installation and Upgrade Procedures](#) located on Cisco.com.

Feature Set Tables

Cisco IOS software is packaged in feature sets consisting of software images, which vary with the hardware platform. Each feature set contains a certain set of Cisco IOS features. Cisco IOS Release 12.3(4)XG supports the same feature sets as Releases 12.3 and 12.3(4)T, but Cisco IOS Release 12.3(4)XG includes new features supported by Cisco 1700 series routers. Cisco IOS Release 12.3(4)XG5 is a rebuild of Cisco IOS Release 12.3(4)XG and includes only bug fixes; it does not include any new features.



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 will likely require an export license. Customer orders can be denied or subject to delay as a result of 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 e-mail to export@cisco.com.

Table 3 lists the features and feature sets supported by legacy images in Cisco IOS Cisco IOS Release 12.3(4)XG, and Table 5 lists the features and feature sets supported by cross-platform images in Cisco IOS Cisco IOS Release 12.3(4)XG. The tables use the following conventions:

- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, “12.4(11)XJ” indicates that the feature was introduced in release 12.4(11)XJ. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.



Note

These feature set tables contain only a list of selected features, which are cumulative for Release 12.3(4)*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 [Cross-Platform Release Notes for Cisco IOS Release 12.3\(4\)T](#) and in Release 12.3(4)T Cisco IOS documentation.

Table 3 Feature List by Cisco 1700 Legacy Feature Set for Cisco 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set		
		IP/ADSL/VOX PLUS	IP/ADSL/VOX/ FW/IDS PLUS IPSEC 3DES	IP/ADSL/IPX/ AT/IBM/VOX/ FW/IDS PLUS IPSEC 3DES
Four-Wire Mode over SHDSL	12.4(11)XJ	Yes	Yes	Yes

Table 4 Feature List by Cisco 1700 Legacy Feature Set for Cisco 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set					
		IP	IP/ADSL	IP/ADSL PLUS	IP/ADSL/ IPX/AT/ IBM PLUS	IP/ADSL/FW/ IDS PLUS IPSEC 3DES	IP/ADSL/IPX/ AT/IBM/FW/ IDS PLUS IPSEC 3DES
Four-Wire Mode over SHDSL	12.4(11)XJ	No	Yes	Yes	Yes	Yes	Yes

Table 5, Part 1 Feature List by Cross-Platform Feature Set for Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set				
		ADVANCED IP SERVICES	SP SERVICES	ENTERPRISE SERVICES	ADVANCED ENTERPRISE SERVICES	IP BASE
Four-Wire Mode over SHDSL	12.4(11)XJ	Yes	Yes	Yes	Yes	Yes

Table 5, Part 2 Feature List by Cross-Platform Feature Set for Cisco 1701, 1710, 1711, 1712, 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set		
		ENTERPRISE BASE	ADVANCED SECURITY	IP VOICE ¹
Four-Wire Mode over SHDSL	12.4(11)XJ	Yes	Yes	Yes

1. This image is supported only on Cisco 1751, 1751-V, and 1760 routers.

New and Changed Information

The following sections list new information about Cisco 1700 series routers for Cisco IOS Release 12.3(4)XG. This information also applies to Cisco IOS Releases 12.3(4)XG1, 12.3(4)XG2, 12.3(4)XG3, 12.3(4)XG4, and 12.3(4)XG5.

New Software Features in Cisco IOS Release 12.3(4)XG

The following sections describe new software features supported by Cisco 1700 series routers for Cisco IOS Release 12.3(4)XG.

Four-Wire Mode over SHDSL

The Four-Wire Mode over SHDSL feature adds four-wire support in fixed mode only on a single-port multiline G.SHDSL WIC, or WIC-1SHDSL-V2, to build on the existing features of the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WAN interface card. The Four-Wire Mode for SHDSL feature incorporates the 2.x firmware version and the latest hybrid circuit from Globespan. The four-wire feature of G.991.2 doubles the bandwidth in ATM mode and increases the usable distance over two pairs of wires.

The Four-Wire Mode over SHDSL feature supports ATM in four-wire mode. Embedded Operation Channel (EOC) message support for customer premise equipment (CPE) is performed for 2-wire and 4-wire modes. G.SHDSL process enhancements improve the performance and reduce the memory utilization.

For more details, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xd/gt4wire.htm>

Two-Wire Mode over SHDSL

The Two-Wire Mode over SHDSL feature adds ATM, E1 and T1 support on a single-port multiline G.SHDSL WAN Interface Card (WIC), or WIC-1SHDSL-V2, to build on the existing features of the Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature supported on the 1-port G.SHDSL WAN interface card.

The Two-Wire Mode over SHDSL feature supports ATM, E1 and T1 in 2-wire mode. Embedded Operations Channel (EOC) message support for customer premise equipment (CPE) is done for 2-wire and 4-wire modes and some central office (CO) messages are also supported.

For more details, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xd/gtgs-hdsl.htm>

IETF-Compliant PPP over ATM

The Internet Engineering Task Force (IETF)-Compliant PPP over ATM feature allows you to configure PPP over ATM by using a virtual circuit multiplexed encapsulation mode. This feature complies with IETF RFC 2364, “PPP over ATM Adaptation Layer 5 (AAL5)”.

New Software Features in Release 12.3(4)T

For information regarding features supported in Cisco IOS Release 12.3(4)T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on [Cisco.com](http://www.cisco.com):

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and follow this path:

Service & Support > Technical Documents > Cisco IOS Software > Release 12.3: Release Notes > Cross-Platform Release Notes (Cisco IOS Release 12.3(4)T)

Limitations and Restrictions

The following sections list limitations and restrictions that apply for Cisco IOS Releases 12.4(11)XJ, 12.3(4)XG1, 12.3(4)XG2, 12.3(4)XG3, 12.3(4)XG4, and 12.3(4)XG5.

Four-Wire Mode for SHDSL

- Cisco 1721 router slot numbering issue

The WIC 1SHDSL-V2, being configurable in ATM/T1/E1 modes, takes up a different interface/controller numbering scheme on the Cisco 1721 router. This problem does not apply to the Cisco 1751 or Cisco 1760 routers, as they use a slot/port numbering scheme.

- With WIC 1SHDSL-V2 (DSL controller) in slot 0, the T1/E1 controllers/ATM interfaces (ADSL/SHDSL) will be numbered relative to the DSL controller in slot 0.

Example 1:

Slot 0 – 1SHDSL-V2, slot 1 – MFT-T1/E1

Number Assignment:

controller dsl 0, int atm 0 or contr t1 0 (depending on the mode configured) - for 1SHDSL-V2
controller t1 1 – for MFT-T1

Example 2:

Slot 0 – 1SHDSL-V2, slot 1 – ADSL/SHDSL

Number Assignment:

controller dsl 0, int atm 0 or contr t1 0 (depending on the mode configured) - for 1SHDSL-V2
interface atm 1 – ADSL/SHDSL

- With an ATM or MFT - T1/E1 card in slot 0, the 1SHDSL-V2 in slot 1 will be numbered relative to the ports in slot 0;

Example 1:

Slot 0 – ADSL/SHDSL, slot 1 – 1SHDSL-V2

Number Assignment:

interface atm 0 – for 1SHDSL/ADSL

controller dsl 1, int atm 1 or contr t1 1 (depending on the mode configured) – for 1SHDSL-V2

Example 2:

Slot 0 – 1MFT-T1/E1, slot 1 – 1SHDSL-V2

Number Assignment:

controller t1 0 for 1MFT-T1

controller dsl 1, int atm 1 or contr t1 1 (depending on the mode configured) - for 1SHDSL-V2

Example 1:

Slot 0 – 2MFT-T1/E1, slot 1 – 1SHDSL-V2

Number Assignment:

controller t1 0 & controller t1 1 for 2MFT-T1

controller dsl 2, int atm 2 or contr t1 2 (depending on the mode configured) – for 1SHDSL-V2

If both slots are occupied by controller DSL, the logical interfaces configured on them will take the numbers of the DSL controller seen (which will be the same as the slot numbers).

All logical interfaces (for example, the serial interface created on configuring channel-groups in T1/E1 mode) on WIC-1SHDSL-V2 will have the same number as the controller dsl.

- Dynamic mode change is not supported.

Dynamic mode changes between ATM/T1/E1 are not supported on Cisco 1700 series routers. The router has to be reloaded after saving the new configuration mode in order for the mode change to take effect. Alternatively, the **no mode** command can be issued, and the router should be reloaded with the configurations saved. After the router is reloaded, a new mode can be configured.

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 Cisco IOS Release 12.3(4)T also exist in Cisco IOS Release 12.3(4)XG5. For information on caveats in Cisco IOS Release 12.3(2)T, refer to the *Caveats for Cisco IOS Release 12.3(4)T* document. This document lists severity 1 and 2 caveats and is located on [Cisco.com](http://www.cisco.com).

**Note**

If you have an account with [Cisco.com](http://www.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](http://www.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 - Cisco IOS Release 12.3(4)XG5

- CSCsb24007

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>

- CSCef67682

Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognizes as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

- CSCee45312

Remote Authentication Dial In User Service (RADIUS) authentication can be bypassed on a device that is running certain Cisco IOS software releases and is configured with a fallback method of none. Devices that run other Cisco IOS software releases, are configured for other authentication methods or are not configured with a fallback method of none are not affected. Some configurations using RADIUS, none and an additional method also are not affected.

Cisco has made free software available to address this vulnerability. There are also workarounds available to mitigate the effects. More details can be found in the security advisory at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>

- CSCeg15044

Symptoms: Although there are free tty lines, you cannot establish a Telnet connection, and a “No Free TTYs” error message is generated.

- CSCeh13489

Symptoms: The BGP session is reset if a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length equal to or greater than 255.

- CSCed03333

Symptoms: CBAC sessions are left in sis-closing state due to out-of-order packet handling.

Workaround: None. Lowering the inspect FTP timeout or disabling CEF reduces exposure.

Fix: Bump certain out-of-order packets to process path for catch-up and then drop packets if this is unsuccessful.

- CSCed65778

Certain Cisco IOS software releases, when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

Cisco has made free software available to address these vulnerabilities for all affected customers. There are also workarounds available to mitigate the effects. More details can be found in the security advisory at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml>

- CSCef44699

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

- Attacks that use ICMP “hard” error messages
- Attacks that use ICMP “fragmentation needed and Don't Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
- Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>

- CSCef61610

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

- Attacks that use ICMP “hard” error messages
- Attacks that use ICMP “fragmentation needed and Don't Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
- Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability. This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>

- CSCsa52807

A document titled “ICMP Attacks Against TCP,” which describes how the Internet Control Message Protocol (ICMP) could be used to perform Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP), has been made publicly available through the Internet Engineering Task Force (IETF) Internet Draft process (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which affect only sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages.
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks.
3. Attacks that use ICMP “source quench” messages.

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. There are also workarounds available to mitigate the effects. More details can be found in the security advisory at the following URL:

<http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:

<http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>

- CSCsa54608

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in certain versions of Cisco IOS software is vulnerable to a remotely exploitable buffer overflow condition.

Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

Cisco has made free software available to address this vulnerability. There are also workarounds available to mitigate the effects. More details can be found in the security advisory at the following URL:

http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml

Resolved Caveats - Cisco IOS Cisco IOS Release 12.3(4)XG4

- CSCef68324

Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

Cisco has made free software available to address this vulnerability for all affected customers.

More details can be found in the security advisory that is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml>.

Resolved Caveats - Cisco IOS Cisco IOS Release 12.3(4)XG3

- CSCee67450

BGP error message trackback.

A device running Cisco IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a DoS attack from a malformed BGP packet. Only devices with the command **bgp log-neighbor-changes** configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

Cisco has made free software available to address this problem. Please see the advisory available at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>.

- CSCef43691

L2TPv3 and UTI sessions doing PMTUD vulnerable to spoofed ICMP paks.

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef44225
IPSec (ESP-AH) doing PMTUD vulnerable to spoofed ICMP packets.
See note for CSCef43691 above.
- CSCef60659
More stringent checks required for ICMP unreachable.
See note for CSCef43691 above.
- CSCsa59600
IPSec PMTUD not working [after CSCef44225].
See note for CSCef43691 above.

Resolved Caveats - Cisco IOS Cisco IOS Release 12.3(4)XG2

- CSCdz32659
%SYS-2-MALLOCFAIL: -Process= CDP Protocol.
Many memory allocation failure (MALLOCFAIL) messages may occur for a Cisco Discovery Protocol (CDP) process:

```
%SYS-2-MALLOCFAIL: Memory allocation of -1732547824 bytes failed from x605111F0, pool
Processor, alignment 0
-Process= "CDP Protocol", ipl= 0, pid= 42
-Traceback= 602D5DF4 602D78A0 605111F8 60511078 6050EC88 6050E684 602D0E2C 602D0E18
```


Workaround: To prevent the symptom from occurring again, disable CDP by entering the **no cdp run** global configuration command.

- CSCec59206
Bus error in NAT translating RSHELL packets.
A router may reload unexpectedly because of a bus error when it accesses a low address during the translation of TCP port 514. This is observed on a Cisco router that runs Cisco IOS Release 12.3(5) and that is configured for Network Address Translation (NAT).
Workaround: Prevent the translation of TCP port 514.
- CSCed35253
Router crash due to corrupted data in list with Cisco IOS firewall.
A router may reload unexpectedly after it attempts to access a low memory address.
Workaround: Disable IP Inspect and IDS.
- CSCed40563
Malicious configuration reload neighbor routers by **show cdp entry * protocol** command.
Depending upon configuration, issuing the **show cdp entry * protocol** command may cause a reload of the device.
Workaround: Disable CDP, avoid issuing the command under given circumstances, or upgrade to a fixed version of software.
- CSCed40933
Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.
More details can be found in the security advisory, which is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.
- CSCed78149
A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).
These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:
 1. Attacks that use ICMP "hard" error messages
 2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
 3. Attacks that use ICMP "source quench" messagesSuccessful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.
Multiple Cisco products are affected by the attacks described in this Internet draft.
Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCee08584

Cisco Internetwork Operating System (IOS) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for Cisco's IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.

A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml>

Cisco has made free software upgrades available to address this vulnerability for all affected customers.

- CSCef46191

Unable to telnet.

A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.

Cisco will make free software available to address this vulnerability. Workarounds, identified below, are available that protect against this vulnerability.

The Advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml>

- CSCed93836

Modifications needed to syn rst packet response.

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCin67568

Memory leak in CDP process with long host names.

A Cisco device experiences a memory leak in the CDP process. The device sending CDP packets sends a hostname that is 256 or more characters. There are no problems with a hostname of 255 or fewer characters.

Workaround: Configure the neighbor device to use less than a 256 character hostname, or disable the CDP process with the **no cdp run** global configuration command.

- CSCee47441

CBAC inspection causes software forced reload.

When Cisco IOS Firewall Context-Based Access Control (CBAC) is configured, the router seems to have a software-forced reload caused by one of the inspections processed.

Workaround: There is no workaround.

- CSCec88490

Cosmetic Display CLI Related Issues.

While giving **line-mode 2-wire ?** command in ATM mode on WIC-1SHDSL-V2, the help text displays incorrect mapping between the line number and the pins used.

Workaround: There is no workaround.

- CSCed21034

atmVclTable maps all permanent virtual circuits (PVCs) to all subinterfaces.

Workaround: There is no workaround.

- CSCin82407

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

Resolved Caveats - Cisco IOS Cisco IOS Release 12.3(4)XG1

- CSCeb56909
Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces. The vulnerability is present only in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable. More details can be found in the security advisory posted at <http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.shtml>.
- CSCec77425
Spurious Accesses at mlp_group_swidb.
- CSCec86420
When the **undebg all** privileged EXEC command is entered on a Cisco router, all traffic that passes through an encrypted generic routing encapsulation (GRE) tunnel may stop. This symptom is observed on a Cisco router that is configured with a GRE tunnel that is secured via IP Security (IPSec) and that is using Cisco Express Forwarding (CEF) switching.
Workaround: Reinitialize CEF switching by entering the **no ip cef** global configuration command followed by the **ip cef** global configuration command.
Alternate Workaround: Do not enter the **undebg all** privileged EXEC command. Rather, individually disable each **debug** command.
- CSCed93090
Symptoms: Line-mode CLI does not have option for auto line mode selection.
Conditions: DSL line training stops if digital subscriber line access multiplexer (DSLAM) switches from two-wire to four-wire or four-wire to two-wire mode.
Workaround: Change the customer premise equipment (CPE) line-mode configuration to DSLAM line-mode configuration.
- CSCed14031
EOC message 17 not received by WIC-1SHDSL and WIC-1SHDSL-V2.
EOC message 17 is not received by WIC-1SHDSL and WIC-1SHDSL-V2 even though a certain third party DSLAM sends it periodically. This is because the said DSLAM sends message 11 and message 17 with one 7E in between. The GTI_EOM interrupt is generated by the firmware on two consecutive 7Es. Hence message 17 is not processed by the CPE.
- CSCed81135
Traces appear when WIC-1-SHDSL-V2 connected to ECI DSLAM.

- CSCed68575

Reload triggered in SNMP process.

Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload. The vulnerability is present only in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change, and is resolved with [CSCed68575](#). This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml>

Open Caveats - Cisco IOS Release 12.3(4)XG

- CSCec59868

Controller and interface flapping for sf&ami on T1.

This problem is seen only when two channel-groups are configured with all 24 timeslots being used.

Workaround: When using all 24 timeslots in sf, configure only one channel-group. If two channel-groups are required, use esf.

- CSCec65083

Loopback analog fails in Cisco 1751/1760 router.

This problem is seen only when both CO and CPE are configured for analog loopback. There is no problem when only one end is configured for loopback.

Workaround: Do not configure analog loopback on both CPE and CO simultaneously.

- CSCed41900

E1 4-wire mode line protocol flapping with Annex-B and unframed framing.

Workaround: There is no workaround.

Resolved Caveats - Cisco IOS Release 12.3(4)XG

This section documents possible unexpected behavior by Cisco IOS Release 12.3(4)XG and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec61461

Small percentage of packet drop seen for 64B packet with G.SHDSL.

When smaller packet size (64 B or 128 B) is used, the low-end routers (Cisco 1700 and Cisco 2600 routers) have lower performance.

Workaround: Use large size packets.

- CSCed27956

TCP checks should verify ack sequence number.

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly.

Depending on the application, the connection may get automatically re-established. In other cases,

a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products that contain a TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed38527

TCP checks should verify ack sequence number.

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products that contain a TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

Related Documentation

The following sections describe the documentation available for Cisco 1700 series 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](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>.

Use these release notes with these documents:

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

- [Cisco Feature Navigator](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on [Cisco.com](#) and <http://www.cisco.com/univercd/home/index.htm>:

- *Cross-Platform Release Notes for Cisco IOS Release 12.3(4)T*

On [Cisco.com](#) at:

Products and Solutions > Cisco IOS Software > Cisco IOS Software Releases 12.3 > Instructions and Guides > Release Notes

On <http://www.cisco.com/univercd/home/index.htm> at:

Cisco IOS Software > Cisco IOS Release 12.3 > Release Notes > Cross-Platform Release Notes



Note Cross-Platform Release Notes for Cisco IOS Release 12.3 T are located on [Cisco.com](#) or on <http://www.cisco.com/univercd/home/index.htm> at **Cisco IOS Software > Cisco IOS Release 12.3 > Release Notes > Cisco IOS Release 12.3 T**.

- Product bulletins, field notices, and other release-specific documents at <http://www.cisco.com/univercd/home/index.htm>
- *Caveats for Cisco IOS Release 12.3*
As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3 T.
On [Cisco.com](#) at:
Products & Services > IOS Software > Cisco IOS Software Releases 12.3 > Instructions and Guides > Release Notes > Release Notes for Cisco IOS Release 12.3, Part 5 > Caveats
On <http://www.cisco.com/univercd/home/index.htm> at:
Cisco IOS Software > Cisco IOS Release 12.3 > Release Notes > Caveats
- If you have an account on [Cisco.com](#), you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](#) and click **Products and Solutions > Cisco IOS Software > Cisco IOS Software Releases 12.3 > Troubleshooting > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

These documents are available for Cisco 1700 series routers:

On [Cisco.com](#) at:

Products and Solutions > Routers > Cisco 1700 Series Modular Access Routers

On <http://www.cisco.com/univercd/home/index.htm> at:

Product Documentation > Routers > Modular Access Routers > Cisco 1700 Series Routers

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on [Cisco.com](http://www.cisco.com). If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with [Cisco.com](http://www.cisco.com). If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on [Cisco.com](http://www.cisco.com) by following the directions found at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

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](http://www.cisco.com) at:

Products and Solutions > Cisco IOS Software > Cisco IOS Releases 12.3 > Instructions and Guides

On <http://www.cisco.com/univercd/home/index.htm> at:

Cisco IOS Software > Cisco IOS Release 12.3 > Configuration Guides and Command References

Cisco IOS Release 12.3 Documentation Set Contents

Table 6 lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions > Cisco IOS Software > Cisco IOS Releases 12.3 > Instructions and Guides

On <http://www.cisco.com/univercd/home/index.htm> at:

Cisco IOS Software > Cisco IOS Release 12.3

Table 6 Cisco IOS Release 12.3 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i> 	<ul style="list-style-type: none"> Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2: IBM Networking</i> 	<ul style="list-style-type: none"> 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 6 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Technologies Configuration Guide</i> • <i>Cisco IOS Dial Technologies Command Reference</i> 	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface and Hardware Component Configuration Guide</i> • <i>Cisco IOS Interface and Hardware Component Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i> • <i>Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility</i> 	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice Configuration Library</i> • <i>Cisco IOS Voice Command Reference</i> 	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 6 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Messages</i> 	

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feed-back, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Use this document in conjunction with the documents listed in the [“Related Documentation”](#) section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, BPX, 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, Networking Academy, Network Registrar, *Packet*, 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. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007, Cisco Systems, Inc. All rights reserved..

