



Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.3(2)XC

September 29, 2003

These release notes describe new features and significant software components for the Cisco 1700 series routers that support the Cisco IOS Release 12.3(2)T, up to and including Release 12.3(2)XC. 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 12.3\(2\)T](#) located on [Cisco.com](#) and the Documentation CD.

For a list of the software caveats that apply to Release 12.3(2)XC, see the “Caveats” section on [page 9](#) and [Caveats for Cisco IOS Release 12.3\(2\)T](#). The online caveats document is updated for every maintenance release and is located on [Cisco.com](#) and the Documentation CD.

Contents

These release notes include the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 8](#)
- [Limitations, page 8](#)
- [Caveats, page 9](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation, page 12](#)
- [Obtaining Technical Assistance, page 13](#)
- [Obtaining Additional Publications and Information, page 15](#)



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

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

System Requirements

This section describes the system requirements for Release 12.3(2)XC and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 5](#)
- [Determining the Software Version, page 5](#)
- [Upgrading to a New Software Release, page 5](#)
- [Feature Set Tables, page 6](#)

Memory Requirements

Table 1 describes the memory requirements for the Cisco IOS feature sets supported by the Cisco IOS Release 12.3(2)XC on the Cisco 1700 series routers.

Table 1 Recommended Memory for the Cisco 1700 Series Routers¹—Legacy Images

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1710 ²	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	64 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, and 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	96 MB
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751- V, and 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, and Cisco 1760	Cisco 1700 IOS IP	IP	c1700-y-mz	16 MB	48 MB

Table 1 Recommended Memory for the Cisco 1700 Series Routers¹—Legacy Images (continued)

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, and Cisco 1760	Cisco 1700 IOS IP/ADSL/IPX/AT/IBM PLUS	IP/ADSL/IPX/AT/IBM PLUS	c1700-bnr2sy7-mz	16 MB	64 MB
Cisco 1701, Cisco 1711, Cisco 1712, Cisco 1721, Cisco 1751-V, and 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, and 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, and 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

1. The WIC-4ESW is supported only on the Cisco 1721, 1751, 1751-V, and 1760 routers.

2. The Cisco 1710 router does not support Security Device Manager (SDM).

Table 2 Recommended Memory for the Cisco 1700 Series Routers¹—Cross-Platform Images

Platform	Image Name	Feature Set ²	Image	Flash Memory	DRAM
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, and Cisco 1760	Cisco 1700 IOS IP BASE	IP BASE	c1700-ipbase-mz	16 MB	64 MB
Cisco 1751, Cisco 1751-V, and Cisco 1760	Cisco 1700 IOS IP VOICE	IP VOICE	c1700-ipvoice-mz	32 MB	96 MB

Table 2 Recommended Memory for the Cisco 1700 Series Routers¹—Cross-Platform Images (continued)

Platform	Image Name	Feature Set ²	Image	Flash Memory	DRAM
Cisco 1701, Cisco 1721, Cisco 1751, Cisco 1751-V, and Cisco 1760	Cisco 1700 IOS ENTERPRISE BASE	ENTERPRISE BASE	c1700-entbase-mz	16 MB	64 MB
Cisco 1701, Cisco 1711, Cisco 1712, Cisco 1721, Cisco 1751, Cisco 1751-V, and 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, and 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, and 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, and 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, and Cisco 1760	Cisco 1700 IOS ADVANCED ENTERPRISE SERVICES	ADVANCED ENTERPRISE SERVICES	c1700-adventerprisek9-mz	32 MB	96 MB

1. The WIC-4ESW is supported only on the Cisco 1721, 1751, 1751-V, and 1760 routers.

2. Refer to the product bulletin "[Cisco IOS Software Release 12.3 Mainline and 12.3T Feature Sets for Cisco 1700 Series Routers](#)."

Hardware Supported

Cisco IOS Release 12.3(2)XC supports the following Cisco 1700 series routers:

- Cisco 1701 router
- Cisco 1710 router
- Cisco 1711 router
- Cisco 1712 router
- Cisco 1720 router
- Cisco 1721 router
- Cisco 1751 and 1751-V routers
- Cisco 1760

The Cisco 1701, Cisco 1710, Cisco 1711, Cisco 1712, Cisco 1720, and Cisco 1721 routers run data images only. The Cisco 1751, Cisco 1751-V, and Cisco 1760 routers run data or data-and-voice images, providing digital and analog voice support. The Cisco 1711 and Cisco 1712 routers run select IPsec Triple Data Encryption Standard (3DES) images only (the Cisco 1700 IOS IP/ADSL/IPX/AT/IBM/FW/IDS PLUS IPSEC 3DES, the Cisco 1700 IOS IP/ADSL/FW/IDS PLUS IPSEC 3DES, the Cisco 1700 Advanced Security, and the Cisco 1700 Advanced Enterprise Services images).

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1700 series routers, which are available on [Cisco.com](http://www.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 [Cisco.com](http://www.cisco.com), 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 which version of Cisco IOS software is 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.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (C1700-NY-MZ), Version 12.3(2)XC, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synchronized to technology version 12.3(1.6)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to the *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 12.3(2)XC supports the same feature sets as Releases 12.3 and 12.3(2)T, but Release 12.3(2)XC includes new features supported by the Cisco 1700 series routers.



Caution

The 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 an e-mail to export@cisco.com.

Table 3 through Table 6 lists the feature and feature sets supported in the Cisco IOS Release 12.3(2)XC.

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, “12.3(2)XC” means that the feature was introduced in 12.3(2)XC. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.



Note

These feature set tables contain only a selected list of features, which are cumulative for Release 12.3(2)*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\(2\)T](#) and Release 12.3(2)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
WIC-4ESW (4-Port Ethernet Switch WIC)	12.3(2)XC	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
WIC-4ESW (4-Port Ethernet Switch WIC)	12.3(2)XC	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Cross-Platform Feature Set for Cisco 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set
		IP VOICE
WIC-4ESW (4-Port Ethernet Switch WIC)	12.3(2)XC	Yes

Table 6, Part 1 Feature List by Cross-Platform Feature Set for Cisco 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set				
		ADVANCED IP SERVICES	SP SERVICES	ENTERPRISE SERVICES	ADVANCED ENTERPRISE SERVICES	IP BASE
WIC-4ESW (4-Port Ethernet Switch WIC)	12.3(2)XC	Yes	Yes	Yes	Yes	Yes

Table 6, Part 2 Feature List by Cross-Platform Feature Set for Cisco 1721, 1751, 1751-V, and 1760 Routers

Feature	In	Feature Set	
		ENTERPRISE BASE	ADVANCED SECURITY
WIC-4ESW (4-Port Ethernet Switch WIC)	12.3(2)XC	Yes	Yes

New and Changed Information

The following sections list the new hardware features supported by the Cisco 1700 series routers for Release 12.3(2)XC.

New Hardware Features in Release 12.3(2)XC

The following sections describe the new hardware features supported by the Cisco 1700 series routers for Release 12.3(2)XC.

WIC-4ESW (4-Port Ethernet Switch WIC)

The WIC-4ESW (4-Port Ethernet Switch WAN interface card [WIC]) is a new four-port managed 10/100 Base-T Layer 2 switch in a WIC form factor. The switch supports IEEE 802.1D spanning tree algorithm and can be used to connect upto four LANs or up to 16 IEEE 802.1Q based virtual LANs.

New Software Features in Release 12.3(2)T

For information regarding the features supported in the Cisco IOS Release 12.3(2)T, refer to the Cross-Platform Release Notes and New Feature Documentation links at the following location on 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 click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.3: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.3(2)T)

Limitations

The following sections describe limitations concerning the new hardware and software features supported by the Cisco 1700 series routers for Release 12.3(2)XC.

WIC-4ESW (4-Port Ethernet Switch WIC)

The following features are not supported on WIC-4ESW card:

- VLAN trunking protocols (server and client modes, and transparent mode, Version 2) and Spanning Tree Protocol (STP) backbone fast
- STP portfast Bridge Protocol Data Unit (BPDU) guard
- STP uplink fast
- STP Root Guard
- STP Unidirectional Link Detection (UDLD)
- Port security
- Protected port

- 802.1x port-based authentication
- Storm control
- Switched Port Analyzer (SPAN)
- Internet Group Management Protocol (IGMP) Snooping
- 802.1P priority override
- MAC address table commands
- EtherChannel
- Enable or disable per port based on unknown unicast or multicast flooding
- Multicast groups
- IP multicast support
- Cisco Group Management Protocol (CGMP) client, CGMP fast-leave
- Dynamic access ports
- Dynamic trunk protocol
- Dynamic VLANs
- Voice VLANs
- General Attribute Registration Protocol (GARP), GARP Multicast Registration Protocol (GMRP), and GARP VLAN Registration Protocol (GVRP)
- Cisco Inter-Switch Link (ISL) tagging (the chip does not support ISL)
- Layer 3 onboard switching
- Monitoring of VLANs
- Multi-VLAN ports network port
- Shared STP instances
- VLAN-based SPAN
- VLAN Query Protocol (VQP)
- VTP pruning protocol
- Web-based management interface
- Remote Monitoring (RMON)

Caveats

Caveats describe unexpected behavior or defects in the 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(2)T are also in Release 12.3(2)XC. For information on caveats in Cisco IOS Release 12.3(2)T, refer to the [Caveats for Cisco IOS Release 12.3\(2\)T](#) document. This document lists severity 1 and 2 caveats; the documents are located on Cisco.com and the Documentation CD.

**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 - Release 12.3(2)XC

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

- 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 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>.

- 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 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>.

Open Caveats for Release 12.3(2)XC

- Only one WIC-4ESW card can be installed on a Cisco 1700 series router.
- Currently the WIC-4ESW card is supported only on Cisco 1721, 1751, 1751-V, and 1760 routers.
- The WIC-4ESW card cannot be used in a voice interface card (VIC) slot.
- If WIC-4ESW is used with a Cisco IOS image that does not support it, the Link LED does not light, and an error message appears, indicating an unrecognized WIC. This does not damage the router or the WIC-4ESW card. The following error message is displayed:

```
“00:00:05 PQUICC-1-UNKNOWN_WIC:PQUICC(0), WIC card has an unknown ID of 0xFF.”
```
- The router cannot use TFTP over the Cisco WIC-4ESW Ethernet connection until the router completes the boot process.
- This interface is not supported in the ROM Monitor; therefore, a TFTP download cannot be performed by using the interface in ROM Monitor mode.
- The 10/100 Fast Ethernet interfaces support TFTP download in ROM monitor mode. We suggest you connect the 10/100 Fast Ethernet interface to the side of the network that provides the image.
- ConfigMaker does not recognize the WIC-4ESW card.
- The WIC-4ESW switches packets between switch ports at line rates of 10 Mbps or 100 Mbps, including VLAN traffic. Inter-VLAN traffic and routed traffic that require processing by the host CPU are limited to 10 Mbps (full duplex), because the CPU Ethernet port is operating at 10 Mbps.

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](http://www.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 12.3 and apply to Release 12.3(2)XC. They are located on [Cisco.com](http://www.cisco.com) and the Documentation CD (under the heading Service & Support):

- To reach the [Cross-Platform Release Notes for Cisco IOS Release 12.3\(2\)T](#), click this path:

Technical Documents: [Cisco IOS Software: Release 12.3: Release Notes: Cisco IOS Release 12.3\(2\)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 12.3* and *Caveats for Cisco IOS Release 12.3(2)T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.3, click this path:

Technical Documents: [Cisco IOS Software: Release 12.3: Caveats](#)



Note

If you have an account with [Cisco.com](#), you can also use the Bug Toolkit to find selected 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 the 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 [Cisco.com](#), 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](http://www.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](http://www.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](http://www.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](http://www.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](http://www.cisco.com) registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

[Cisco.com](http://www.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](http://www.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](http://www.cisco.com). To access [Cisco.com](http://www.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](http://www.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](http://www.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.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

<http://www.cisco.com/go/packet>

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private Internets and Intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

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

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)
partnership relationship between Cisco and any other company. (0/11R)

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