



Release Notes for the Catalyst 3750, 3560, 3550, 2970, 2955, 2950, 2950 LRE, and 2940 Switches, Cisco IOS Release 12.1(19)EA1c

April 21, 2004

Cisco IOS Release 12.1(19)EA1c runs on these switches:

- Catalyst 3750
- Catalyst 3560
- Catalyst 3550
- Catalyst 2970
- Catalyst 2955
- Catalyst 2950
- Catalyst 2950 LRE
- Catalyst 2940



Note

Use these release notes with the previous Cisco IOS Release 12.1(19)EA1 release notes for information on these specific switch platforms.



Note

Running Cisco IOS Release 12.1(19)EA1c in a Catalyst 3750 switch stack that has other stack members running Cisco IOS Release 12.1(19)EA1 is not a supported configuration. We strongly recommend upgrading the entire switch stack to Cisco IOS Release 12.1(19)EA1c if at least one stack member is running this release.

These release notes include important information about this release and any limitations, restrictions, and caveats that apply to it. See the [“Related Documentation” section on page 11](#) for links to the switch documentation on Cisco.com.



Corporate Headquarters:

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Contents

This document has the following sections:

- [System Requirements, page 2](#)
- [New Features, page 5](#)
- [Resolved Caveats for All Switches, page 7](#)
- [Resolved Caveats for Catalyst 3750, 3560, and 2970 Switches, page 8](#)
- [Resolved Caveats for Catalyst 3750 Switches, page 8](#)
- [Open Cisco IOS Caveats for Catalyst 3750 and 3560 Switches, page 8](#)
- [Related Documentation, page 11](#)
- [Obtaining Documentation, page 11](#)
- [Obtaining Technical Assistance, page 12](#)
- [Obtaining Additional Publications and Information, page 13](#)

System Requirements

The system requirements are described in these sections:

- [“Hardware Supported” section on page 2](#)
- [“Cluster Compatibility” section on page 4](#)
- [“Software Compatibility” section on page 5](#)

Hardware Supported

[Table 1](#) lists the hardware supported by this software release.

Table 1 Catalyst 2940, 2950, 2950 LRE, 2955, 2970, 3550, 3560, and 3750 Hardware Supported

Hardware	Description
Catalyst 2940-8TT-S	8 10/100 Ethernet ports and 1 10/100/1000 Ethernet port
Catalyst 2940-8TF-S	8 10/100 Ethernet ports, 1 SFP ¹ module slot, and 1 100BASE-FX port
Catalyst 2950-12	12 10/100 Ethernet ports
Catalyst 2950-24	24 10/100 Ethernet ports
Catalyst 2950C-24	24 10/100 Ethernet ports and 2 100BASE-FX ports
Catalyst 2950G-12-EI	12 10/100 Ethernet ports and 2 GBIC ² module slots
Catalyst 2950G-24-EI	24 10/100 Ethernet ports and 2 GBIC module slots
Catalyst 2950G-24-EI-DC	24 10/100 Ethernet ports and 2 GBIC module slots with DC-input power
Catalyst 2950G-48-EI	48 10/100 Ethernet ports and 2 GBIC module slots
Catalyst 2950ST-8 LRE	8 LRE ³ ports, 2 10/100/1000 Ethernet ports ⁴ , and 2 SFP module slots
Catalyst 2950ST-24 LRE	24 LRE ports, 2 10/100/1000 Ethernet ports ⁴ , and 2 SFP module slots

Table 1 Catalyst 2940, 2950, 2950 LRE, 2955, 2970, 3550, 3560, and 3750 Hardware Supported (Continued)

Hardware	Description
Catalyst 2950ST-24 LRE 997	24 LRE ports, 2 10/100/1000 Ethernet ports ⁴ , and 2 SFP module slots with DC-input power
Catalyst 2950SX-24	24 10/100 Ethernet ports and 2 1000BASE-SX ports
Catalyst 2950SX-48-SI	48 10/100 Ethernet ports and 2 1000BASE-SX ports
Catalyst 2950T-24	24 10/100 Ethernet ports and 2 10/100/1000 Ethernet ports ⁵
Catalyst 2950T-48-SI	48 10/100 Ethernet ports and 2 10/100/1000 Ethernet ports
Catalyst 2955C-12	12 10/100 ports and 2 MM ⁶ 100BASE-FX ports
Catalyst 2955S-12	12 10/100 ports and 2 SM ⁷ 100BASE-LX ports
Catalyst 2955T-12	12 10/100 ports and 2 10/100/1000 Ethernet ports ⁴
Catalyst 2970G-24T	24 10/100/1000 Ethernet ports
Catalyst 2970G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots
Catalyst 3550-12G	10 GBIC-based Gigabit Ethernet slots and 2 10/100/1000 Ethernet ports
Catalyst 3550-12T	10 10/100/1000 Ethernet ports and 2 GBIC-based Gigabit Ethernet slots
Catalyst 3550-24	24 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet slots
Catalyst 3550-24-DC	24 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet slots with DC-input power
Catalyst 3550-24-FX	24 100BASE-FX ports and 2 GBIC-based Gigabit Ethernet slots
Catalyst 3550-24PWR	24 10/100 Cisco prestandard PoE ⁸ ports and 2 GBIC-based Gigabit Ethernet slots
Catalyst 3550-48	48 10/100 Ethernet ports and 2 GBIC-based Gigabit Ethernet slots
Catalyst 3560-24PS	24 10/100 PoE ports and 2 SFP module slots
Catalyst 3560-48PS	48 10/100 PoE ports and 4 SFP module slots
Catalyst 3750G-12S	12 SFP module slots
Catalyst 3750-24TS	24 10/100 Ethernet ports and 2 SFP module slots
Catalyst 3750G-24T	24 10/100/1000 Ethernet ports
Catalyst 3750G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots
Catalyst 3750-48TS	48 10/100 Ethernet ports and 4 SFP module slots
Catalyst 3750-24PS	24 10/100 PoE ports and 2 SFP module slots
Catalyst 3750-48PS	48 10/100 PoE ports and 4 SFP module slots

1. SFP = small form-factor pluggable

2. GBIC = Gigabit Interface Converter

3. LRE = Long-Reach Ethernet

4. The 10/100/1000 ports on a Catalyst 2950 LRE or Catalyst 2955T-12 switch operate at 10 or 100 Mbps in either full- or half-duplex mode and at 1000 Mbps only in full-duplex mode.

5. The 10/100/1000 interfaces on the Catalyst 2950T-24 switch do not support the **half** keyword in the **duplex** command.

6. MM = multimode

7. SM = single mode

8. PoE = Power over Ethernet

Cluster Compatibility

This section describes how to choose command and standby command switches when a cluster consists of a mixture of Catalyst switches. When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch. [Table 2](#) lists the cluster capabilities and Cisco IOS releases for the switches. The switches are listed from highest- to lowest-end switch.
- If you are managing the cluster through CMS, and the command switch is running Cisco IOS Release 12.1(19)EA1 or later, the switch that has the latest software release does not have to be the command switch. It is also not required that the highest-end switch in your cluster be the command switch if the command switch is running Cisco IOS Release 12.1(19)EA1 or later.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750 switch, all standby command switches must be Catalyst 3750 switches.

Table 2 Switch Software and Cluster Capability

Switch	Cisco IOS Release	Cluster Capability
Catalyst 3750	12.1(11)AX or later	Member or command switch
Catalyst 3560	12.1(19)EA1b or later	Member or command switch
Catalyst 3550	12.1(4)EA1 or later	Member or command switch
Catalyst 2970	12.1(11)AX or later	Member or command switch
Catalyst 2955	12.1(12c)EA1 or later	Member or command switch
Catalyst 2950	12.1(5.2)WC(1) or later	Member or command switch
Catalyst 2950 LRE	12.1(11)JY or later	Member or command switch
Catalyst 2940	12.1(13)AY or later	Member or command switch
Catalyst 3500 XL	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (8-MB switches)	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (4-MB switches)	11.2(8.5)SA6 (recommended)	Member switch only ¹
Catalyst 1900 and 2820	9.00(-A or -EN) or later	Member switch only

1. Catalyst 2900 XL (4-MB) switches appear in the front-panel and topology views of the Cluster Management Suite (CMS). However, CMS does not support configuration or monitoring of these switches.

CMS is not forward-compatible on command switches running Cisco IOS 12.1(14)EA1 and earlier. This means that if a member switch is running a release that is newer than the release running on the command switch, the new features are not available on the member switch. If the member switch is a new device running a release that is later than the release on the command switch, and if the command switch is running a release earlier than Cisco IOS Release 12.1(19)EA1, the command switch cannot recognize the member switch, and the Front Panel view displays it as an unknown device. You cannot configure any parameters or generate a report through CMS for that member; instead, you must launch the Device Manager application to configure and to obtain reports for that member.

If you have a cluster with switches that are running different versions of Cisco IOS software, features added on the latest release might not be reflected on switches running the older releases. For example, if you start CMS on a Catalyst 2900 XL switch running Cisco IOS Release 11.2(8)SA6, the windows and functionality can be different from a switch running Cisco IOS Release 12.0(5)WC(1) or later.

Some early Cisco IOS releases do not support clustering.

For more information about clustering and CMS, refer to the software configuration guide.

Software Compatibility

For information about the recommended platforms for web-based management, operating systems and browser support, and CMS plug-in guidelines, refer to the “Getting Started with CMS” chapter of the software configuration guide.

Windows

This release uses a CMS plug-in to run CMS. You can download the latest CMS plug-in for Windows from this URL:

http://www.cisco.com/cgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=windows&version=1.1

Solaris

This release uses a CMS plug-in that replaces the Java plug-in. You can download the latest CMS plug-in for Solaris from this URL:

http://www.cisco.com/cgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=solaris&version=1.1

New Features

These sections describe the new supported hardware and the new software features provided in this release:

- “New Hardware Features” section on page 5
- “New Software Features” section on page 6

New Hardware Features

For a list of all supported hardware, see the “Hardware Supported” section on page 2.

New Software Features

Cisco IOS Release 12.1(19)EA1c contains these features:

- Ability to provide power to connected Cisco prestandard and IEEE 802.3af-compliant powered devices from all Catalyst 3750-24PS, 3750-48PS, 3560-24PS, and 3560-48PS switch 10/100 Ethernet ports if the switch detects that there is no power on the circuit.
- The Catalyst 3750-24PS and 3560-24PS switches can provide 15.4 W of power on each 10/100 port; the Catalyst 3750-48PS and 3560-48PS switches can provide 15.4 W of power to any 24 of the 48 10/100 ports, or any combination of ports can provide an average of 7.7 W of power at the same time, up to maximum switch power output of 370 W.
- Automatic detection and power budgeting; the switch maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.



Note

The Cisco IP Phone 7970G can operate in low- and high-power modes. For high-power mode and full functionality, we recommend that you use an external power adapter. The phone functions if power is provided by Cisco prestandard or IEEE 802.3af PoE, but it has reduced power, and the display is at half brightness. The Catalyst 3550, 3560, and 3750 switches can provide 15.4 W per port. However, this release does not support CDP enhancements to allow negotiation with the Cisco IP Phone 7970G to cover its wider power range.

Refer to the *Cisco IP Phone 7970 Administration Guide for Cisco CallManager* for details.



Note

On PoE switches, CDP messages enable the switch to refine the power consumption of Cisco powered devices with more accuracy than what is available by using generic IEEE Classes.

On 48-port PoE switches, CDP allows the switch to optimize the available 370 W budget of PoE across Cisco powered devices.

- CMS support for these features:
 - The option to install CMS on your computer rather than to download it from the cluster every time you start a CMS session.



Note

CMS is downloaded to your browser each time you launch CMS. You can increase the speed at which CMS loads by permanently installing CMS on your PC or workstation. Select **CMS > Installation and Distributions**, and click **Install**. CMS is installed locally and will load faster the next time that you launch it.

- A feature bar, which offers networking features to configure and reports, graphs, and statistics to display. These options were previously on the menu bar, which is now dedicated to CMS service options. You can choose features from menus on the Features tab or search for them on the Search tab.

- Device-specific online help. Help topics appear below labels that name the devices to which the information applies. Topics appear only for the networking features in the cluster.
- This release uses a CMS plug-in for Solaris and Windows that replaces the Java plug-in.



Note You must download the latest CMS plug-in to run CMS for this release.

You can download the latest plug-ins from these URLs:

http://www.cisco.com/cgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=windows&version=1.1

http://www.cisco.com/cgi-bin/Support/ClusterMgmtSuite/cms_plugin_redirect.cgi?platform=solaris&version=1.1

For more information about new CMS features, click **Help > What's New** from the online help.

For a detailed list of key features for this software release, refer to the software configuration guide for your switch.

Resolved Caveats for All Switches

These resolved caveats are applicable to all Catalyst switches running this release:

- CSCec82728

A transient spanning tree loop no longer occurs when rapid-PVST+, MSTP/RSTP is running and the root bridge has aged out.

- CSCed27956

A vulnerability in Transmission Control Protocol specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in much shorter time than was previously publicly discussed. This can lead to a Denial of Service attack. Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated session, which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (e.g., router, switch, computer) and not to the sessions that are only passing through the device (e.g., transit traffic that is being routed by a router).

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>.

- CSCed29169

The IP Internet Group Management Protocol (IGMP) report expiration timer no longer expires in 1 second, no matter how you configured the IGMP query-max-response-time setting. Having the timer set to 1 second, regardless of how it was configured, sometimes caused multicast receiver ports to be prematurely removed from their multicast group on a given VLAN.

- CSCed38527

A vulnerability in Transmission Control Protocol specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in much shorter time than was previously publicly discussed. This can lead to a Denial of Service attack. Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated session, which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (e.g., router, switch, computer) and not to the sessions that are only passing through the device (e.g., transit traffic that is being routed by a router).

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>.

- CSCed58872

The topology change counter now operates in multiple spanning-tree (MST) mode.

Resolved Caveats for Catalyst 3750, 3560, and 2970 Switches

This resolved caveat is applicable to these switches:

- CSCec50040

Using the **show controllers ethernet-controller <interface-id> [phy]** privileged EXEC command on a 1000BASE-T copper port or on an SFP module port no longer causes the link to go down or to go up and down continuously.

Resolved Caveats for Catalyst 3750 Switches

These resolved caveats are applicable to these switches:

- CSCed33857

When the switch is operating in multiple STP (MSTP) mode, stack member switches now forward traffic that belongs to newly created VLANs on an EtherChannel or trunk.

- CSCed50935

When Dynamic Host Configuration Protocol (DHCP) snooping is enabled, the software no longer forwards all routed IP packets after a stack master election.

Open Cisco IOS Caveats for Catalyst 3750 and 3560 Switches

This is the severity 3 Cisco IOS configuration caveat:

- CSCed09484

When a type 1 Token Ring patch cable is connected to a PoE port, these syslog messages appear every 10 seconds:

- 00:01:06: %ILPOWER-7-DETECT: Interface Fa1/0/1: Power Device detected: Cisco PD
- 00:01:06: %ILPOWER-5-POWER_GRANTED: Interface Fa1/0/1: Power granted
- 00:01:06: %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error,
- Interface Fa1/0/1: Power Controller reports power Tstart error detected

There is no workaround. However, when a valid link partner is connected to the PoE port, it operates normally and without user intervention.

Which Software Files to Download from Cisco.com

New software releases are posted on Cisco.com and are also available through authorized resellers. These tables list the software filenames for this software release:

- [Table 3](#) (Catalyst 3750)
- [Table 4](#) (Catalyst 3560)
- [Table 5](#) (Catalyst 3550)
- [Table 6](#) (Catalyst 2970)
- [Table 7](#) (Catalyst 2955)
- [Table 8](#) (Catalyst 2950)
- [Table 9](#) (Catalyst 2950 LRE)
- [Table 10](#) (Catalyst 2940)



Note

We recommend that you download the combined .tar file that contains the IOS image and the CMS files. For instructions on how to upgrade your switch, refer to the Cisco IOS Release 12.1(19)EA1 release notes for your switch platform. For Catalyst 3560 switches, refer to the Cisco IOS Release 12.1(19)EA1b release notes.



Caution

For Catalyst 3750 and 2970 switches, this software release includes a bootloader upgrade. The bootloader can take up to 1 minute to upgrade and occurs the first time that the new software is loaded. Do not power cycle the switch during the bootloader upgrade.



Caution

A bootloader upgrade occurs if you are upgrading Catalyst 2950 switches running Cisco IOS Release 12.1(9)EA1d or earlier to Cisco IOS Release 12.1(11)EA1 or later for both cryptographic and noncryptographic images. A bootloader upgrade occurs if you are upgrading Catalyst 3550 switches from a noncryptographic image to cryptographic image, regardless of the current noncryptographic Cisco IOS Release that is running on the switch. The bootloader can take up to 30 seconds to upgrade. Do not power cycle the switch while you are copying this image to the switch. If a power failure occurs when you are copying this image to the switch, call Cisco Systems immediately.

Table 3 Cisco IOS Software Image Files for Catalyst 3750 Switches

Filename	Description
c3750-i9-tar.121-19.EA1c.tar	Catalyst 3750 SMI Cisco IOS image and CMS files
c3750-i5-tar.121-19.EA1c.tar	Catalyst 3750 EMI Cisco IOS image and CMS files
c3750-i9k2-tar.121-19.EA1c.tar	Catalyst 3750 SMI cryptographic Cisco IOS image and CMS files
c3750-i5k2-tar.121-19.EA1c.tar	Catalyst 3750 EMI cryptographic Cisco IOS image and CMS files

Table 4 Cisco IOS Software Image Files for Catalyst 3560 Switches

Filename	Description
c3560-i9-tar.121-19.EA1c.tar	Catalyst 3560 SMI Cisco IOS image and CMS files
c3560-i5-tar.121-19.EA1c.tar	Catalyst 3560 EMI Cisco IOS image and CMS files
c3560-i9k2-tar.121-19.EA1c.tar	Catalyst 3560 SMI cryptographic Cisco IOS image and CMS files
c3560-i9k2-tar.121-19.EA1c.tar	Catalyst 3560 EMI cryptographic Cisco IOS image and CMS files

Table 5 Cisco IOS Software Image Files for Catalyst 3550 Switches

Filename	Description
c3550-i9q3l2-tar.121-19.EA1c.tar	Catalyst 3550 SMI Cisco IOS image and CMS files
c3550-i5q3l2-tar.121-19.EA1c.tar	Catalyst 3550 EMI Cisco IOS image and CMS file
c3550-i9k2l2q3-tar.121-19.EA1c.tar	Catalyst 3550 SMI cryptographic Cisco IOS image and CMS files
c3550-i5k2l2q3-tar.121-19.EA1c.tar	Catalyst 3550 EMI cryptographic Cisco IOS image and CMS files

Table 6 Cisco IOS Software Image Files for Catalyst 2970 Switches

Filename	Description
c2970-i6l2-tar.121-19.EA1c.tar	Catalyst 2970 EI Cisco IOS image and CMS files
c2970-i6k2l2-tar.121-19.EA1c.tar	Catalyst 2970 EI cryptographic Cisco IOS image and CMS files

Table 7 Cisco IOS Software Image Files for Catalyst 2955 Switches

Filename	Description
c2955-i6q4l2-tar.121-19.EA1c.tar	Catalyst 2955 EI Cisco IOS image and CMS files
c2955-i6k2l2q4-tar.121-19.EA1c.tar	Catalyst 2955 EI cryptographic Cisco IOS image and CMS files

Table 8 Cisco IOS Software Image Files for Catalyst 2950 Switches

Filename	Description
c2950-i6q4l2-tar.121-19.EA1c.tar	Catalyst 2950 SI ¹ and EI Cisco IOS image and CMS files
c2950-i6k2l2q4-tar.121-19.EA1c.tar	Catalyst 2950 EI cryptographic Cisco IOS image and CMS files

1. Switches that support only the SI cannot run the cryptographic image.

Table 9 Cisco IOS Software Image Files for Catalyst 2950 LRE Switches

Filename	Description
c2950lre-i6l2q4-tar.121-19.EA1c.tar	Catalyst 2950 LRE Cisco IOS image and CMS files
c2950lre-i6k2l2q4-tar.121-19.EA1c.tar	Catalyst 2950 LRE cryptographic Cisco IOS image and CMS files

Table 10 Cisco IOS Software Image Files for Catalyst 2940 Switches

Filename	Description
c2940-i6q4l2-tar.121-19.EA1c.tar	Catalyst 2940 Cisco IOS image and CMS files

Related Documentation

These documents provide complete information about the switches and are available at Cisco.com:

- For Catalyst 3750: <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm>
- For Catalyst 3560: <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3560/index.htm>
- For Catalyst 3550: <http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/index.htm>
- For Catalyst 2970: <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/index.htm>
- For Catalyst 2955, 2950, and 2950 LRE:
<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/index.htm>
- For Catalyst 2940: <http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2940/index.htm>

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/index.shtml>

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

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

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

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

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

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

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

- 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://cisco.com/univercd/cc/td/doc/pcat/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. 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/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/ipj>

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

<http://www.cisco.com/en/US/learning/index.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section on page 11.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>

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. (0401R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.