Release Notes for the Catalyst 3750 Switch Cisco IOS Release 12.1(14)EA1

July 2003

The Cisco IOS Release 12.1(14)EA1 runs on all Catalyst 3750 switches. Catalyst 3750 switches support stacking through Cisco StackWise technology. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about this Cisco IOS release and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, refer to the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Determining the Software Version and Feature Set" section on page 4.
- If you are upgrading to a new release, refer to the software upgrade filename for the software version.

For the complete list of Catalyst 3750 switch documentation, see the "Related Documentation" section on page 30.

You can download the switch software from these sites:

- http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

  (for registered Cisco.com users with a login password)
- http://www.cisco.com/public/sw-center/sw-lan.shtml

  (for nonregistered Cisco.com users)

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com (previously Cisco Connection Online [CCO]) in the Cisco IOS software area.

Note If you are upgrading a switch that uses the 802.1X feature, you must re-enable 802.1X after upgrading the software. For more information, see the "Cisco IOS Notes" section on page 20.

CISCO SYSTEMS

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

Contents

This information is in the release notes:

System Requirements

These are the system requirements for this software release:

Hardware Supported

Table 1 lists the hardware supported by this software release.

Table 1 Supported Hardware

Switch	Description
Catalyst 3750G-12S[1]	12 small form-factor pluggable (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
SFP modules	1000BASE-T[1], 1000BASE-SX, 1000BASE-LX and 1000BASE-ZX[1]
Redundant power system	Cisco RPS 300 redundant power system for the Catalyst 3750G-24TS, 3750G-24T, and 3750-48TS switch models (not supported on the Catalyst 3750-24TS switch) Cisco RPS 675 redundant power system for the entire Catalyst 3750 switch family

1. New hardware supported in this release

Software Compatibility

For information about the recommended platforms for web-based management, operating systems and browser support, Java plug-in guidelines and installation procedures, refer to the *Catalyst 3750 Switch Hardware Installation Guide*.

Creating Clusters with Different Releases of Cisco IOS Software

When a cluster consists of a mixture of Catalyst switches, the Catalyst 3750 must be the command switch. The Catalyst 3750 switch can be part of a cluster as a standalone switch or as a switch stack. In a cluster, a switch stack is treated as a single entity.

When the command switch is a Catalyst 3750 switch, all standby command switches must also be Catalyst 3750 switches. The Catalyst 3750 switch that has the latest software should be the command switch. If the command switch is a Catalyst 3750 Gigabit Ethernet switch and the standby command switch is a Catalyst 3750 Fast Ethernet switch, command switch port speeds are reduced if the standby command switch takes over.

Table 2 lists the cluster capabilities and software versions for the switches. The switches are listed in the order of highest to lowest end switch. A lower-end switch cannot be the command switch of a switch listed above it in the table (for example, a Catalyst 2950 switch cannot be the command switch of a cluster that has Catalyst 2970 or Catalyst 3550 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 3550	12.1(4)EA1 or later	Member or command switch
Catalyst 2970	12.1(11)AX or later	Member or command switch
Catalyst 2950	12.1(5.2)WC(1) or later	Member or command switch
Catalyst 2955	12.1(12c)EA1 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.

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

Note The CMS is not forward-compatible, which means that if a member switch is running a software version 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 supported by a software release that is later than the software release on the command switch, the command switch cannot recognize the member switch, and it is displayed as an unknown device in the Front Panel view. 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.

Downloading Software

These are the procedures for downloading software:

- "Determining the Software Version and Feature Set" section on page 4
- "Determining Which Files to Use" section on page 5
- "Upgrading a Switch by Using CMS" section on page 5
- "Upgrading a Switch by Using the CLI" section on page 5
- "Recovering from a Software Failure" section on page 6

Note Before downloading software, read this section for important information.

Determining the Software Version and Feature Set

The Cisco IOS image is stored as a .bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board Flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line displays C3750-I5-M for the enhanced multilayer image (EMI) or C3750-I9-M for the standard multilayer software image (SMI).

Note Although the **show version** output always shows the software image running on the switch (Layer 2 or Layer 2/3), the model name shown at the end of this display is the factory configuration (SMI or EMI) and does not change if you upgrade the software image.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in Flash memory.

Determining Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined .tar file. This file contains both the Cisco IOS image file and the files needed for the CMS. You must use the combined .tar file to upgrade the switch through the CMS. To upgrade the switch through the CLI, use the .tar file and the **archive download-sw** privileged EXEC command.

Table 3 lists the software filenames for this software release.

Table 3 Cisco IOS Software Image Files for Catalyst 3750 Switches

Filename	Description
c3750-i9-tar.121-14.EA1.tar	Cisco IOS SMI image file and CMS files. This image has Layer 2+ and basic Layer 3 routing features including access control lists (ACLs), quality of service (QoS), static routing, and the Routing Information Protocol (RIP).
c3750-i5-tar.121-14.EA1.tar	Cisco IOS EMI image file and CMS files. This image has both Layer 2+ and full Layer 3 routing features (IP unicast routing, IP multicast routing, and fallback bridging). The EMI includes protocols such as the Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), Open Shortest Path First (OSPF) Protocol, and Border Gateway Protocol (BGP).
c3750-i9k2-tar.121-14.EA1.tar	Cisco IOS SMI crypto image file and CMS files. This image has the Kerberos, SSH, and Layer 2+, and basic Layer 3 routing features.
c3750-i5k2-tar.121-14.EA1.tar	Cisco IOS EMI crypto image file and CMS files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.

Upgrading a Switch by Using CMS

You can upgrade switch software by using CMS. From the menu bar, select **Administration > Software Upgrade**. For detailed instructions, click **Help**.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined .tar file to the Catalyst 3750 switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, and if necessary, the TFTP server application, follow these steps:

Step 1 Use Table 3 on page 5 to identify the file that you want to download.

Step 2 Download the software image file.

- If you have a SmartNet support contract, go to this URL and log in to download the appropriate files:

  http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

- If you do not have a SmartNet contract, go to this URL and follow the instructions to register on Cisco.com and download the appropriate files:

  http://www.cisco.com/public/sw-center/sw-lan.shtml

To download the SMI and EMI files, select **Catalyst 3750 software**.

To obtain authorization and to download the crypto software files, select **Catalyst 3750 3DES Cryptographic Software**.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

Step 4 Log in to the switch through the console port or a Telnet session.

Step 5 Ensure that you have IP connectivity to the TFTP server by using this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, refer to the *Catalyst 3750 Switch Software Configuration Guide*.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by using this privileged EXEC command:

```
archive download-sw /overwrite /reload tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in Flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.

For **//***location*, specify the IP address of the TFTP server.

For */directory*/*image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/c3750-i9-tar.121-14.EA1.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

Switch software can be corrupted during an upgrade, by downloading the wrong file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity. You can use the XMODEM protocol to recover from this failure.

For detailed recovery procedures, refer to the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The Express Setup program (See the procedure that follows).
- The setup program (Refer to the *Catalyst 3750 Switch Hardware Installation Guide*.)
- The Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration (Refer to the *Catalyst 3750 Switch Software Configuration Guide*.)
- Manually assigning an IP address (Refer to the *Catalyst 3750 Switch Software Configuration Guide*.)

Note If you are upgrading a switch that uses the 802.1X feature, you must re-enable 802.1X after upgrading the software. For more information, see the "Cisco IOS Notes" section on page 20.

Using Express Setup to Configure a Switch

Express Setup is a browser-based program that you can use to set up and configure the switch. You assign the IP information so that the switch can connect to local routers and the Internet. The IP address is also required if you plan to further configure the switch.

You do not create a username with Express Setup. Express Setup provides the minimum configuration to configure a switch. To create a username for the switch, use the Cluster Management Suite (CMS) or the command-line interface (CLI).

Note To use Express Setup, you must have Cisco IOS Release 12.1(14)EA1 or later running on your switch.

This section provides a quick step-by-step setup procedure for a standalone switch and includes these steps:

Caution Do not start Express Setup when there are any devices connected to the switch or connect a switch that is already in Express Setup mode to any device other than the PC or workstation that is being used to configure it. The switch acts as a DHCP server during the Express Setup procedure, and only the PC or workstation connected to the switch after Express Startup is started should receive a DHCP address from the switch.

Before using Express Setup to configure a switch, refer to the switch hardware installation guide for this information:

- Removing the switch and AC power cord from the shipping container
- Getting an Ethernet (Category 5) straight-through cable to connect the switch to your PC or workstation
- Powering on the switch

Note The illustrations in this section show the Catalyst 2940 switch, but the Mode button, LEDs, and switch ports are similar on your switch.

Starting Express Setup

Before starting Express Setup, verify that the switch has passed the power-on self-test (POST). The SYST and STAT LEDs are green if the switch has passed POST. For information about troubleshooting a POST failure, refer to the switch hardware installation guide. You cannot start Express Setup until POST has completed.

Follow these steps to start the Express Setup program:

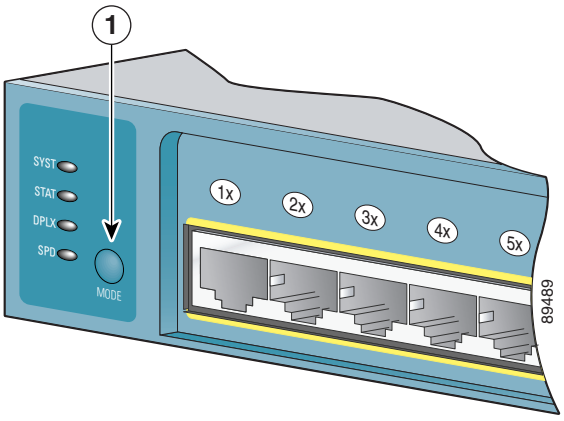
Step 1 Verify that no devices are connected to the switch.

Step 2 Press and hold the Mode button, as shown in Figure 1, until the four LEDs next to the Mode button turn green. This takes approximately 2 seconds.

Note If all of the Mode LEDs begin to blink after you have held the Mode button for 2 seconds, a configuration already exists on the switch and the switch cannot go into Express Setup mode. Release the button. For more information, see the "Clearing the Switch IP Address and Configuration" section on page 13.

Caution If you continue to hold the button for 8 more seconds, the switch configuration is deleted and the switch reloads.

Figure 1 Starting Express Setup



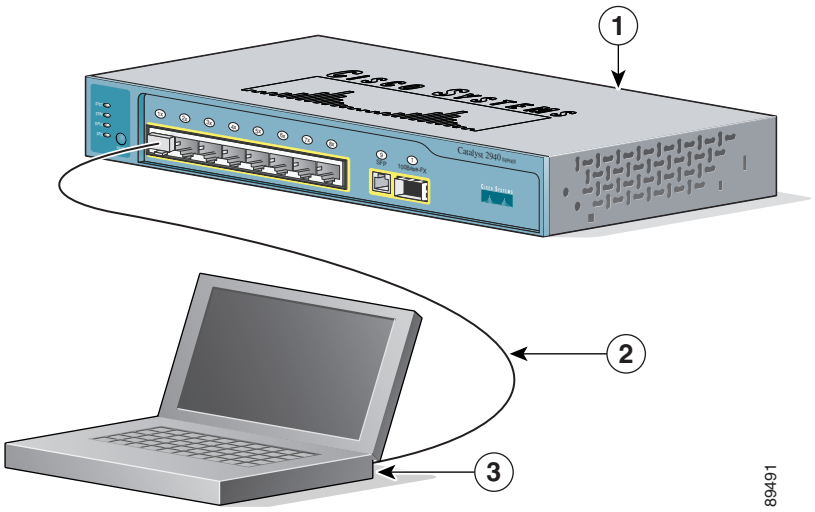
1	Mode button

Step 3 When the LEDs turn green, release the Mode button.

Step 4 Connect the Ethernet cable (not included) to a 10/100 Ethernet port on the front panel of the switch, as shown in Figure 2.

Caution Do not connect the switch to any device other than the PC or workstation being used to configure it.

Figure 2 Connecting the Switch and PC or Workstation Ethernet Ports



1	Switch	**3**	PC or workstation
2	Ethernet cable		

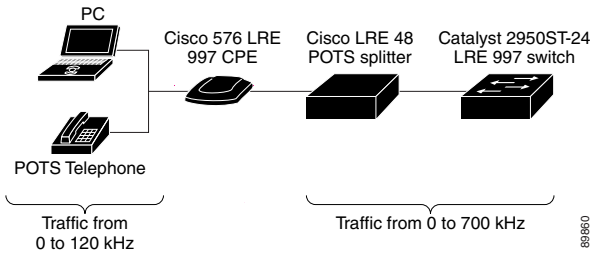
Step 5 Connect the other end of the cable to the Ethernet port on the PC or workstation.

Verify that the port status LED on the switch Ethernet port is green.

Step 6 Wait approximately 30 seconds *after* the port LED turns green, and launch a web browser on your PC or workstation.

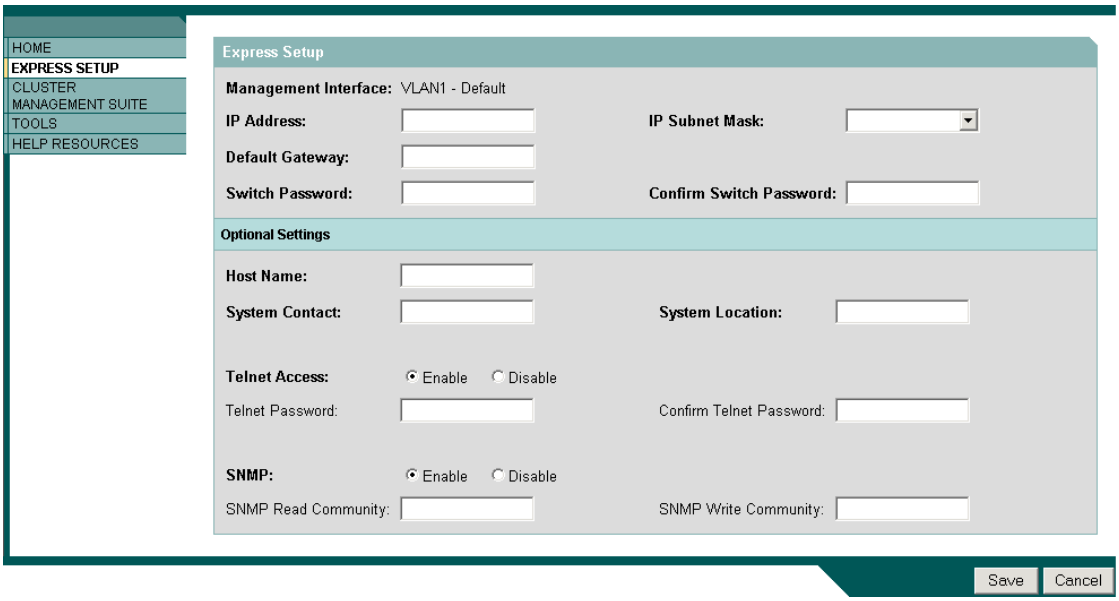
Step 7 Enter the IP address **10.0.0.1** in the browser, as shown in Figure 3, and press **Enter**.

Figure 3 Entering the IP Address



The Express Setup home page appears, as shown in Figure 4.

Figure 4 Express Setup Home Page



If the Express Setup does not run, or the Express Setup home page does not appear in your browser:

- Did you wait 30 seconds after connecting the switch and PC or workstation before entering the IP address in your browser?

  If not, wait 30 seconds and re-enter **10.0.0.1** and press **Enter.**

- Did you enter the wrong address in your web browser, or is there an error message displayed in the browser window?

  Re-enter **10.0.0.1** and press **Enter**.

- Did you connect a crossover instead of a straight-through Ethernet cable between an Ethernet port of the switch and the Ethernet port of the PC or workstation, as shown Figure 2?

  If not, reconnect the cable to the Ethernet port on the switch and PC or workstation. Wait 30 seconds before entering **10.0.0.1** in the browser.

- Did you verify that POST successfully ran before starting Express Setup?

  If not, make sure that only the SYST and STAT LEDs are green before pressing the Mode button to begin Express Setup.

Note The rest of this section explains how to configure a switch by using the Express Setup web page. To configure the switch by using the CLI-based setup program, refer to the switch hardware installation guide.

Configuring the Switch Settings

The Management Interface field displays *VLAN1-Default*. This is the management interface through which you manage the switch and to which you assign IP information.

Follow these steps to configure your switch with Express Setup:

Step 1 Contact your system administrator and obtain the IP address, the IP subnet mask, and the default gateway for your switch.

Step 2 Enter the IP address of the switch in the **IP Address** field.

Step 3 Click the drop-down arrow in the **IP Subnet Mask** field, and select an **IP Subnet Mask**.

Step 4 Enter the IP address for the default gateway in the **Default Gateway** field.

A gateway (router or dedicated network device) is a system that connects a network on one subnet to one or more networks on a different subnet.

Note You must specify a default gateway if the management workstation and the switch are on different IP segments.

Step 5 Enter your password in the **Switch Password** field.

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow embedded spaces at the beginning or end.

Step 6 Enter your password again in the **Confirm Switch Password** field.

You do not enter a username for the switch. After the switch is configured with an IP address, you can use CMS to configure a username.

Step 7 (Optional) Enter a host name for the switch in the **Host Name** field. The host name is limited to 31 characters; embedded spaces are not allowed.

Step 8 (Optional) Enter the name of your system contact in the **System Contact** field. This identifies the system administrator for the switch or network.

Step 9 (Optional) Enter your system location in the **System Location** field. This identifies the physical location of the switch.

Step 10 (Optional) Click **Enable** in the **Telnet Access** field if you are going to use Telnet to manage the switch by using the CLI. If you enable Telnet access, you must enter a Telnet password:

a. Enter a password in the **Telnet Password** field. The Telnet password can be from 1 to 25 alphanumeric characters, is case sensitive, allows embedded spaces, but does not allow embedded spaces at the beginning or end.

b. Enter the Telnet password again in the **Confirm Telnet Password** field.

Step 11 (Optional) Click **Enable** to configure Simple Network Management Protocol (SNMP). Enable SNMP only if you plan to manage switches by using Cisco Works or another SNMP-based network-management system.

If you enable SNMP, you must enter a community string in either the **SNMP Read Community** field, the **SNMP Write Community** field, or both. SNMP community strings authenticate access to MIB objects. Embedded spaces are not allowed in SNMP community strings. If you set the SNMP read community, users can access MIB objects, but cannot modify them. If you set the SNMP write community, users can access and modify MIB objects.

Step 12 Click **Save** to save your settings to the switch, or click **Cancel** to clear your settings.

After you save your settings, the switch exits Express Setup mode. Your switch is now configured with the new IP address. You can install the switch in your production network.

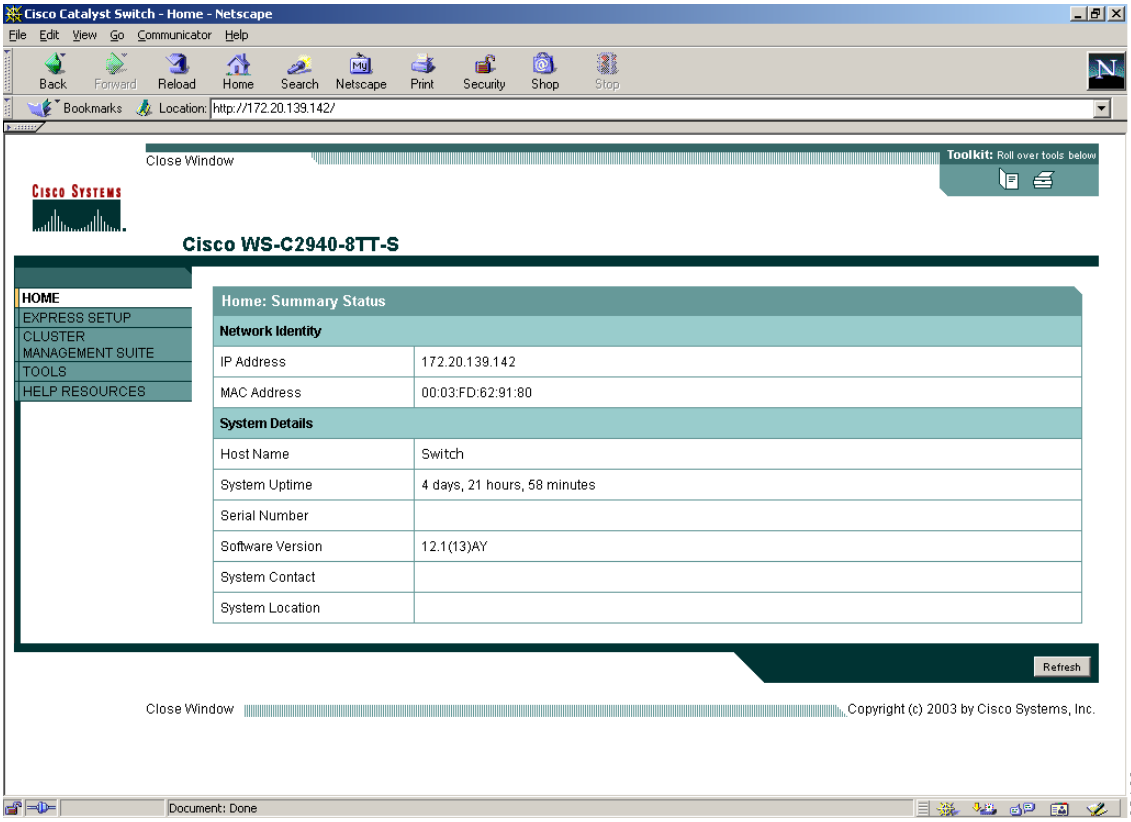
Verifying Switch IP Address (Optional)

After you have installed the switch in your network, follow these steps to verify the IP address configured on your switch:

Step 1 Launch a web browser on a PC or workstation that is connected the network.

Step 2 Enter the IP address of your switch (for example: **172.20.139.142**.) The switch home page appears, as shown in Figure 5.

Figure 5 Switch Home Page



Re-Running Express Setup

If you did not click Save at the end of the "Configuring the Switch Settings" section on page 10 section, you can re-run Express Setup by clicking **Express Setup** on the Switch home page.

If you have entered a wrong IP address or need to change the IP address of your switch, you can clear the IP address on your switch by following the steps in the "Clearing the Switch IP Address and Configuration" section on page 13.

Clearing the Switch IP Address and Configuration

If you have configured a new switch with a wrong IP address, or all the switch LEDs start blinking when you are trying to enter Express Setup mode, you can clear the IP address that is configured on the switch.

Note This procedure clears the IP address and all configuration information stored on the switch. Do not follow this procedure unless you want to completely reconfigure the switch.

To clear the IP address and the switch configuration information, follow these steps:

Step 1 Press and hold the Mode button, as shown in Figure 1 on page 8.

The switch LEDs begin blinking after about 2 seconds.

Step 2 Continue holding down the Mode button. The LEDs stop blinking after 8 additional seconds, and then the switch reboots.

Note These steps only works on a previously configured switch.

Where to Go Next

After you have saved your configuration to the switch, you can install the switch (refer to the switch hardware installation guide) or further configure it (refer to the switch software configuration guide).

New Features

These are the new supported hardware and the new software features provided this release:

- "New Hardware Features" section on page 13
- "New Software Features" section on page 13

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(14)EA1 contains these new features or enhancements:

- Express Setup for quickly configuring a switch for the first time with basic IP information, contact information, switch and Telnet passwords, and SNMP information through a browser-based program. For more information, see Using Express Setup to Configure a Switch, page 7.
- IEEE 802.1S Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic

- Rapid per-VLAN Spanning-Tree plus (Rapid-PVST+) based on IEEE 802.1W Rapid Spanning Tree Protocol (RSPT) for rapid convergence of the spanning tree upon network failure and topology changes
- Trusted boundary to detect the presence of a Cisco IP phone, to trust the Class of Service (CoS) value received, and to ensure port security
- Automatic quality of service (QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring ingress and egress queues (voice over IP only)
- Link Aggregation Control Protocol (LACP) to facilitate the automatic creation of EtherChannels by exchanging packets between Ethernet interfaces. LACP is defined in IEEE 802.3AD.
- Support for these new security features:
  - 802.1X with per-user access control lists for providing different levels of network access and service to an 802.1X-authenticated user
  - 802.1X with VLAN assignment for restricting 802.1X-authenticated users to a specified VLAN
  - 802.1X with port security for controlling access to 802.1X ports
  - 802.1X with voice VLAN to detect the presence of a Cisco IP phone and permit the IP phone access to voice VLAN irrespective of the authorized or unauthorized state of the port
  - 802.1X with guest VLAN to provide limited services to clients that might not be 802.1X-compliant
- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- VLAN1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch CPU continues to send and receive control protocol frames.
- Port security enhancements, including support for CISCO-PORT-SECURITY-MIB, trunk ports and sticky MAC addresses, and the maximum number of secure MAC addresses specified in the SDM template
- Automatic media-dependent interface crossover (Auto MDIX) capability on 10/100 and 10/100/1000 Mbps interfaces that enables the interface to automatically detect the required cable connection type (straight through or crossover) and configure the connection appropriately
- Support for standard and extended IP access control lists (ACLs) and extended MAC ACLs in the inbound direction on Layer 2 interfaces (port ACLs).
- In-band management access through SNMPv3. SNMP version 3 AuthPriv mode requires the cryptographic (encrypted) version of the switch software image SMI and EMI.
- A new show interface capability privileged EXEC command to display configuration capability of a port
- Support for the 10/100/1000BASE-T and 1000BASE-ZX SFP modules
- Border Gateway Protocol (BGP) Version 4 (requires the enhanced multilayer image)
- Policy-based routing (PBR) for configuring defined policies for traffic flows
- Support for the Catalyst 3750G-12S
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic [that is, supports encryption] versions of the SMI and EMI)
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic [that is, supports encryption] versions of the SMI and EMI)

- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device

For a detailed list of key features for this software release, refer to the *Catalyst 3750 Switch Software Configuration Guide*.

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

These are the limitations and restrictions:

- "Cisco IOS Limitations and Restrictions" section on page 15
- "Cluster Limitations and Restrictions" section on page 18
- "CMS Limitations and Restrictions" section on page 19

Cisco IOS Limitations and Restrictions

These limitations apply to Cisco IOS configuration:

- Non-reverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in some other VLAN. Because unnecessary traffic is sent on the trunk port, it needlessly reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member on a trunk port in at least one VLAN, this problem for the non-RPF traffic occurs. (CSCdu25219)
- If a bridge group contains a VLAN that has a static MAC address configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group. The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified with the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the replicate option. For a remote SPAN session, there is no workaround. This is a hardware limitation. (CSCdy72835)
- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the remote SPAN (RSPAN) VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the encapsulation replicate option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround. This is a hardware limitation. (CSCdy81521)

- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- A static IP address might be removed when the previously acquired Dynamic Host Configuration Protocol (DHCP) IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted without a configuration (no config.text file in Flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176)
- The Catalyst 3750 switch treats frames received with mixed encapsulation (802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and causes the LED to blink amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP-option software-forwarded traffic is sometimes leaked unnecessarily on a trunk port. Suppose the trunk port in question is member of an IP multicast group in VLAN X, but it is not a member in VLAN Y. In VLAN Y, there is another port that has membership to the group, and VLAN Y is the output interface for the multicast route entry corresponding to the group. IP options traffic received on an input interface VLAN (other than VLAN Y) is unnecessarily sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y (even though the port has no group membership in VLAN Y). There is no workaround. (CSCdz42909)
- Known unicast (secured addresses) are flooded within a bridge group under these conditions: If secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group, non-IP traffic destined to the secure addresses is flooded within the bridge group. The workaround is to disable fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group** *bridge-group* interface configuration command. Another workaround is to disable port security on all ports in all VLANs participating in fallback bridging by using the **no switchport port-security** interface configuration command. (CSCdz80499)
- When you use the **ip access-group** interface configuration command with a router ACL to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)
- SNAP-encapsulated IP packets are dropped without an error message being reported at the interface. The switch does not support SNAP-encapsulated IP packets. There is no workaround. (CSCdz89142)
- The switch does not create an adjacency table entry when the ARP timeout value is 15 seconds and the ARP request times out.

  The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)

- If a Catalyst 3750 switch stack is connected to a designated bridge and the root port of the switch stack is on a different switch than the alternate root port, changing the port priority of the designated ports on the designated bridge has no effect on the root port selection for the Catalyst 3750 switch stack. There is no workaround. (CSCea40988)
- A route map that contains an ACL with a DSCP clause cannot be applied to a Layer 3 interface. The Catalyst 3750 rejects this configuration and issues an error message saying that the route map is unsupported. There is no workaround. (CSCea52915)
- If the stack master is power cycled immediately after entering the **ip mroute** global configuration command, there is a slight chance that this configuration change will be lost after the stack master switchover. This occurs because the stack master did not have time to propagate the running configuration to all the stack members before it was powered down. This problem might also affect other configuration commands. There is no workaround. (CSCea71255)
- If there are a large number of SVIs, routes, or both on a fully populated nine-member switch stack, an error message like the following might appear when you reload the switch stack or add a switch to the stack:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 4252 bytes failed from 0x179C80, alignment 0
  Pool: I/O Free: 77124  Cause: Memory fragmentation
  Alternate Pool: None Free: 0  Cause: No Alternate pool
  ```

  This error message indicates a temporary memory shortage that normally recovers by itself. You can verify that the switch stack has recovered by entering the **show cef line** user EXEC commend and verifying that the line card states are `up` and `sync`. No workaround is required because the problem is self-correcting. (CSCea71611)
- During periods of very high traffic, when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session. (CSCea72326)
- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue. The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- A Gigabit Ethernet connection between a SGMII (Serial Gigabit Media Independent Interface) port (3/4, 7/8, 11/12, 15/16, 19/20, and 23/24) and an Intel Pro/1000T Server Adapter NIC might loose connectivity on the Catalyst 3750G-24T and Catalyst 3750G-24TS switches. The link activates correctly, but might subsequently stop exchanging data. This is an Intel product defect. The workaround is to use RGMII (Reduced Gigabit Media Independent Interface) ports (1/2, 5/6, 9/10, 13/14, 17/18, and 21/22) instead of SGMII ports. Alternatively, use the **speed 1000** interface configuration command to force the speed of the port to 1000. (CSCea77032)
- When an IP phone is connected to the switch, the Port VLAN ID (PVID) and the Voice VLAN ID (VVID) both learn its MAC address. However, after dynamic MAC addresses are deleted, only the VVID relearns the phone MAC address. MAC addresses are deleted manually or automatically for a topology change or when port security or an 802.1X feature is enabled or disabled. There is no workaround. (CSCea80105)
- After changing the access VLAN on a port that has 802.1X enabled, the IP phone address is removed. Because learning is restricted on 802.1X capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)

- The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)
- A Catalyst 3750 switch might not be able to pass Vine (Advanced Research Projects Agency) ARPA frames over bridge groups. The workaround is to use Subnetwork Access Protocol (SNAP) frames. (CSCeb10032)
- If a 10/100BASE-T port configured for forced 100 mbps full-duplex mode is connected to a link partner that is auto-negotiating, the link partner comes up in 100 mbps full-duplex mode. However, if the same link partner is connected to a Gigabit port configured for forced 100 mbps full-duplex mode, the link comes up in 100 mbps half-duplex mode. The reason for this inconsistent behavior is that the 10/100 port auto-negotiates even if both speed and duplex mode are fixed, whereas the Gigabit port does not. This is a hardware limitation. No workaround is necessary. (CSCeb14068)
- On Catalyst 3750 switches running Cisco IOS 12.1(14)EA1 software, some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)
- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail. The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

Cluster Limitations and Restrictions

These limitations apply to cluster configuration:

- When there is a transition from the cluster active command switch to the standby command switch, Catalyst 1900, Catalyst 2820, and Catalyst 2900 4-MB switches that are cluster members might lose their cluster configuration. You must manually add these switches back to the cluster. (CSCds32517, CSCds44529, CSCds55711, CSCds55787, CSCdt70872)
- When a Catalyst 2900 XL or Catalyst 3500 XL cluster command switch is connected to a Catalyst 3550 or to a Catalyst 3750 switch, the command switch does not find any cluster candidates beyond the Catalyst 3550 or the Catalyst 3750 switch if it is not a member of the cluster. You must add the Catalyst 3550 or the Catalyst 3750 switch to the cluster. You can then see any cluster candidates connected to it. (CSCdt09918)
- If both the active command-switch and the standby command switch fail at the same time, the cluster is not automatically recreated. Even if there is a third passive command switch, it might not recreate all cluster members because it might not have all the latest cluster configuration information. You must manually recreate the cluster if both the active and standby command switches simultaneously fail. (CSCdt43501)

CMS Limitations and Restrictions

These limitations apply to CMS configuration:

- Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not enter commas when entering multiple DNS names in the IP Configuration tab of the IP Management window in CMS.
- Access control entries (ACEs) that contain the **host** keyword precede all other ACEs in standard access control lists (ACLs). You can reposition the ACEs in a standard ACL with one restriction: No ACE with the **any** keyword or a wildcard mask can precede an ACE with the **host** keyword.
- CMS performance degrades if the Topology View is open for several hours on a Solaris machine. The cause might be a memory leak. The workaround is to close the browser, reopen it, and launch CMS again. (CSCds29230)
- If you are printing a Topology View or Front Panel View that contains many devices and are running Solaris 2.6 with JDK1.2.2, you might get an *Out of Memory* error message. The workaround is to close the browser, re-open it, and launch CMS again. Before you perform any other task, bring up the view that you want to print, and click **Print** in the **CMS** menu. (CSCds80920)
- If a PC running CMS has low memory and CMS is running continuously for 2 to 3 days, the PC runs out of memory. The workaround is to relaunch CMS. (CSCdv88724)
- When a VLAN or a range of VLANs is already configured and you specify a VLAN filter for a SPAN session, the current configuration for that session is overwritten with the new entry. Although the CLI appends new entries after the existing ones, CMS recreates the whole session, overwrites the current entry, and provides only a single VLAN filter per entry. The workaround is to use the CLI. It is the only method for specifying multiple VLANs for filtering in a SPAN session. (CSCdw93904)
- When you add a new member with a username and password that is different from the existing cluster members username and password, CMS produces an exception error because of an authentication failure. The workaround is to add the new member without any username and password. When the new member is added to the cluster, remove the existing username and password from the Username and Password fields, enter a new username and password, and then apply it to all cluster members. (CSCdz07957)
- When the Link Graphs application has run for hours displaying packet drop and error information, sometimes the X-axis crosses the Y-axis at a negative y value instead of at y = 0. This condition occurs with all supported operating systems, browsers, and Java plug-ins. There is no workaround. (CSCdz32584)
- CMS temporarily halts while starting. This occurs only when using Windows 98 and these combinations of Netscape browser and Java run-time environment:
  - Netscape 4.75 and JRE 1.3.1 or 1.4.0
  - Netscape 6.2 and JRE 1.3.1

  The workaround is to click once outside of the CMS Window. CMS then proceeds. (CSCdz72175)
- The SNMP dialog box changes size after clicking Apply or Refresh. This behavior has no affect on SNMP functionality. There is no workaround. (CSCdz84255)
- When you enable log scaling for link graphs, the Y-axis scale becomes illegible. There is no workaround. (CSCdz81086)

- The CMS window does not return to full size after you resize elements when using Netscape version 6.xx on Solaris and Linux. This is a Netscape browser problem. There is no workaround. (CSCea01179)
- CMS files that are downloaded from the switch to the local client machine are not cached on the local drive. As the result. the CMS files are downloaded every time CMS is invoked. There is no workaround. (CSCea26211)
- CMS sometimes halts after you click Apply when using Netscape 4.7 on the Japanese version of Windows 98 or Windows ME. The workaround is to use Microsoft Internet Explorer or Netscape 6.0 or later. (CSCea27408)
- The icons on the CMS menu toolbar become blank. This can happen when you unlock the PC with CMS running or interrupt the in-display screen saver. The workaround is to resize the CMS browser window so that the screen refreshes. (CSCea80753)
- Changing the password or current authentication while CMS is running causes HTTP requests to fail.

  The workaround is to close all browser sessions and then relaunch CMS. (CSCeb33995)

Important Notes

These are the important notes related to this software release:

- "Switch Stack Notes" section on page 20
- "Cisco IOS Notes" section on page 20
- "Cluster Notes" section on page 21
- "CMS Notes" section on page 21

Switch Stack Notes

These notes apply to switch stacks.

- Always power off a switch before adding or removing it from a switch stack.
- Cisco IOS Release 12.1(14)EA1 is not backward-compatible with Cisco IOS Release 12.1(11)AX. If you add a switch running 12.1(14)EA1 to an existing stack running Cisco IOS Release 12.1(11)EA1, the added switch changes to version-mismatch state and cannot be configured for normal operation. You can either downgrade the new switch to the same version running on the stack's active switch or upgrade the entire stack.

Cisco IOS Notes

This note applies to Cisco IOS.

- The 802.1X feature in Cisco IOS Release 12.1(14)EA1 is not fully backward-compatible with the same feature in Cisco IOS Release 12.1(11)AX. If you are upgrading a switch running Cisco IOS Release 12.1(11)AX that has 802.1X configured, you must re-enable 801.1X after the upgrade by using the **dot1x system-auth-control** global configuration command. This global command does not exist in Cisco IOS Release 12.1(11)AX. Failure to re-enable 801.1X weakens security because some hosts can then access the network without authentication.

Cluster Notes

There are no cluster configuration notes to report.

CMS Notes

These notes apply to CMS configuration:

- If you use CMS on Windows 2000, it might not apply configuration changes if you change the enable password from the CLI during your CMS session. You have to restart CMS and enter the new password when prompted. Platforms other than Windows 2000 prompt you for the new enable password when it is changed.
- CMS does not display QoS classes that are created through the CLI if these classes have multiple match statements. When using CMS, you cannot create classes that match more than one match statement. CMS does not display policies that have such classes.
- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.add.com*:84), you must enter *http://* as the URL prefix. Otherwise, you cannot launch CMS.
- Within an ACL, you can change the sequence of ACEs that have the **host** keyword. However, because such ACEs are independent of each other, the change has no effect on the way the ACL filters traffic.
- If you use the Netscape browser to view the CMS GUI and you resize the browser window while CMS is initializing, CMS does not resize to fit the window.

  Resize the browser window again when CMS is not busy.
- CMS does not start if the temporary directory on your computer runs out of memory. This problem can occur because of a bug in the 1.2.2 version of the Java plug-in. The plug-in creates temporary files in the directory whenever it runs CMS, and the directory eventually runs out of plug-in space.

  The workaround is to remove all the jar_cache*.tmp files from the temporary directory. The path to the directory is different for different operating systems:

  Solaris: /var/tmp
  Windows NT and Windows 2000: \TEMP
  Windows 95 and 98: \Windows\Temp
- In the Front Panel view or the Topology view, CMS does not display error messages in read-only mode for these switches:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Cisco IOS Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Cisco IOS Release 12.1(6)EA1 or earlier

  In the Front Panel view, if the switch is running one of the previously listed software releases, the device LEDs do not appear. In the Topology view, if the member is a Long-Reach Ethernet (LRE) switch, the customer premises equipment (CPE) connected to the switch does not appear. The Bandwidth and Link graphs also do not appear in these views.

  To view switch information, you need to upgrade the member switch software. For information about upgrading switch software, see the "Downloading Software" section on page 4.

Open Caveats

These are the open caveats with possible unexpected activity in this software release:

Open Cisco IOS Caveats

These are the severity 3 Cisco IOS configuration caveats:

- CSCdz30046

  When multicast VLAN registration (MVR) groups are added or deleted, the receiver port that joined the groups after the addition still receives traffic even after the group is deleted. The correct behavior is that MVR data traffic to the group should stop flowing to the receiver port immediately after the **no mvr group** *ip-address* global configuration command is entered.

  The workaround is to disable MVR by using the **no mvr** global configuration command and then to re-enable it by using the **mvr** command. Add and delete the groups that have problems by using the **mvr group** *ip-address* and the **no mvr group** *ip-address* global configuration commands.

- CSCea26207

  If the stack master is reloaded immediately after adding multiple VLANs, the new stack master might fail.

  The workaround is to wait a few minutes after adding VLANs before reloading the stack master.

- CSCea75390

  When two RSPAN sessions are active at the same time, packets might swap VLAN IDs during periods of very high traffic. Packets with swapped VLAN IDs can be egressed spanned on VLAN 1.

  There is no workaround.

- CSCea84802

  While booting up a nine-member switch stack with a large number of SNMP traps enabled, some of the stack members might not come up fully and become operational. There are two possible scenarios:

  – The stack member stays in the initializing state. Use the **show switch** user EXEC command to detect this condition. Normally a switch joining the switch stack transitions from `Initializing` to `Ready` within 1 minute.

  – The stack member comes up in the ready state, but all ports on the stack member remain in the linkdown state even though link partners indicate a linkup state.

  The workaround is to reboot the whole switch stack using one of these methods:

  – Use the **reload** privileged EXEC command on the stack master.

  – Power cycle the stack master.

- CSCea90131

  Under the these conditions, the Catalyst 3750 might report a false security violation after an 802.1X supplicant is authenticated and assigned a new VLAN by the RADIUS server:

  – 802.1X, port security, and voice VLAN are configured on a stack member port.

  – Maximum number of secure addresses have been learned on the port before it is authenticated.

  - The VLAN assigned by the RADIUS server is different than the access VLAN configured on the port.

  This problem does not prevent traffic from being forwarded to the 802.1X client, but the **show port-security** privileged EXEC command might indicate that the port is `SecureDown` when it is actually `SecureUp` and forwarding traffic correctly.

  The workaround is to restart the interfaces that appear to be out of sync by using the **shutdown** and then **no shutdown** interface configuration commands.

- CSCeb01226

  Gigabit Ethernet ports might have FCS errors when operating at Gigabit speeds on the Catalyst 3750G-24T and Catalyst 3750G-24TS switches. The FCS error rate for this condition is very low.

  The workaround is to restart the ports by using the **shutdown** and then **no shutdown** interface configuration commands.

- CSCeb13978

  A Distance Vector Multicast Routing Protocol (DVMRP) tunnel can remain down after reloading the switch.

  There is no workaround.

- CSCeb14406

  Distance Vector Multicast Routing Protocol (DVMRP) does not forward packets correctly.

  There is no workaround.

- CSCeb29898

  After booting up a switch stack that has more than 300 VLANs and the maximum number of static EtherChannel groups (12), all interfaces that are part of an EtherChannel might stay down. This occurs because the remote switch detects an EtherChannel misconfiguration and disables its ports. This problem can occur in either PVST+ or Rapid-PVST+ mode.

  The workaround is to restart the EtherChannel ports or configure automatic recovery:

  - Use the **shutdown** and **no shutdown** interface configuration commands on the remote switch to restart all err-disabled interfaces
  - Use the **errdisable recovery cause channel-misconfig** global configuration command to enable automatic link recovery on the remote switch, and use the **errdisable recovery interval** global configuration command to configure a short recovery interval.

- CSCeb35263

  After switches are added to or removed from a switch stack, the reconfiguration processes can defer normal CPU processes, such as CLI command handling, and make them unresponsive. The duration of the reconfiguration process depends on the size and nature of the running configuration, but the delay is not significant until the switch configuration exceeds several thousand lines. After the update finishes, CLI responsiveness returns.

  There is no workaround other than removing commands from the switch configuration.

- CSCeb35422

  On a voice VLAN port with both 802.1X and port security enabled, dynamic secure addresses might not get deleted when the port is changed from multihost mode to single-host mode. This means that addresses learned in the multihost mode are still allowed after changing to single-host mode. This problem occurs under the following conditions:

  - The port is in authorized state.

  - The port learns the MAC address of multiple hosts.
  - VLAN assignment is not enabled for the authorized host.

  The workaround is to disable and then re-enable port security on the port.

- CSCeb37125

  If a switch stack is running fallback bridging and the switches in the switch stack have routed ports in the bridge-group, fallback bridging might not work. This occurs when the TCAM is full and a switch is added or deleted from the switch stack.

  The workaround is to stop traffic to free up space in TCAM and then to reload the whole switch stack. Then enable the traffic 1 minute after the switch stack comes back up.

- CSCeb40267

  If a Catalyst 3750 switch loaded with Cisco IOS Release 12.1(14)EA1 software is added to a switch stack running Cisco IOS Release 12.1(11)AX software, the stack member changes to version mismatch (as expected). If an SNMP application traverses the CISCO-FLASH-MIB, a stack member in version mismatch state can fail.

  The workaround is to avoid traversing the CISCO-FLASH-MIB while the switch stack is being upgraded from Cisco IOS Release 12.1(11)AX to Cisco IOS Release 12.1(14)EA1.

- CSCeb42949

  A Catalyst 3750 switch does not work with the User Registration Tool (URT). The PC attempting to connect to the network can log in successfully, but is not allowed to pass traffic after the port is moved to the user VLAN. The MAC address for that device shows BLOCKED.

  There is no workaround.

- CSCeb42953

  If an IP phone is connected to a port on the stack master, and 802.1X port security and voice VLAN are configured on the port, disabling port security causes the IP phone MAC address to be deleted from the MAC address table on all stack members. The MAC address table on the stack master retains the phone MAC address.

  There is no workaround.

- CSCeb54159

  If an interface on a Catalyst 3750 switch is mapped to queue-set 2, and you disable and then re-enable multilayer QoS globally using the **mls qos** global configuration command, the interface is no longer mapped to the correct egress queue-set.

  The workaround is to reconfigure the interface queue-set by using the **no queue-set** interface configuration command followed by the **queue-set 2** interface configuration command.

- CSCeb56226

  If an 802.1X port is configured for forced-unauthorized port control mode and voice VLAN, after you remove the voice VLAN and disable 802.1X on the port, the port no longer passes traffic.

  The workaround is to restart the port by using the **shutdown** and then the **no shutdown** interface configuration commands.

- CSCeb66720

  When CDP is disabled on a stack member interface and that interface is converted to a routed port or switch port, CDP is re-enabled on the stack member interfaces. Having CDP enabled on a stack member but not on the stack master can cause the 802.1X voice VLAN and inline power features to fail on the stack member.

  The workaround is to enable and then disable CDP on the interface.

- CSCeb69078

  Executing remote commands on a Catalyst 3750-12S switch that is unpacking and copying a new software image to Flash memory can cause the software upgrade to fail.

  The workaround is to reload the switch to re-enable Flash operations, and then repeat the software upgrade procedure.

Open CMS Caveats

These are the severity 3 CMS configuration caveats:

- CSCdz01037

  CMS fails when a switch is running the crypto software image and the vty lines have been configured to use only secure shell (SSH) using the **transport input ssh** and **line vty 0 15** global configuration commands.

  The workaround is to allow SSH and Telnet access through the vty lines by using the **transport input ssh telnet** and **line vty 0 15** global configuration commands.

- CSCeb05183

  The Port Settings table displays meaningless information in the columns for interface description and duplex cells. This problem occurs for some of the Catalyst 2820 and Catalyst 1900 switches.

  There is now workaround.

- CSCeb23334

  CMS does not validate configuration values for STP port priority before applying them to the switch. When invalid values are applied, the attempt fails silently without a warning message. This applies to all switches running Cisco IOS Release 12.1 or later.

  There is no workaround. Make sure that configuration values are valid.

- CSCeb23416

  CMS does not validate configuration values for STP port path cost before applying them to the switch. When invalid values are applied, the attempt fails silently without a warning message. This applies to all switches running Cisco IOS Release 12.1 or later.

  There is no workaround. Make sure that configuration values are valid for the switch type.

- CSCeb23592

  CMS does not validate configuration values for STP bridge parameters before applying them to the switch. When invalid values are applied, the attempt fails silently without a warning message. This applies to all switches running Cisco IOS 12.1 or later.

  There is no workaround. Make sure that configuration values are valid.

- CSCeb25630

  The Link Graphs bar chart for Packet Drops & Errors might display erroneous errors for Ethernet interfaces.

  The workaround is to use the **show interfaces** or **show interfaces counter** privileged EXEC commands command.

- CSCeb38514

  Sometimes a switch stack icon disappears from the topology view. This can occur if one of the switch stack members goes down or a switch stack member is disconnected from the stack.

  The workaround is to close the CMS browser and launch CMS again.

- CSCeb38967 LOTR and TRS

  When CMS is operating in read-only mode, an error is reported if help is launched from the QoS Graph dialog box.

  There is no workaround.

- CSCeb40625

  CMS does not apply shaped bandwidth weights that are invalid. Shaped weights are invalid if the sum of their reciprocals is greater than 1 and the weight of a queue is 0.

  There is no workaround.

Resolved Caveats

These are the caveats that have been resolved in this release.

- "Cisco IOS Caveats Resolved in Release 12.1(14)EA1" section on page 26
- "Cisco CMS Caveats Resolved in Release 12.1(14)EA1" section on page 29

Cisco IOS Caveats Resolved in Release 12.1(14)EA1

These Cisco IOS caveats were resolved in Release 12.1(14)EA1:

- CSCdy29217

  After the stack master failover and when the previous stack master rejoins the stack, some Layer 3 configuration on routed port interfaces belonging to the previous stack master are no longer lost (for example, the IP address, bridge groups, and so forth). This problem previously occurred under these conditions:

  - When the configuration of the switch stack has been modified but not saved.
  - The stack master fails, and a new switch in the switch stack is elected to become the new stack master.
  - The previous stack master rejoins the switch stack.
  - There is at least one port on the previous stack master physically configured as a routed port with some Layer 3 configuration.

- CSCdy40828

  If the switch stack is a designated bridge in the LAN and another switch is connected to the switch stack through redundant links and has one of these redundant ports in a blocking state, the spanning-tree state topology is now the same after configuration changes in the LAN. For example, if the root bridge has ports that go down and then come back up, the switch stack remains a designated bridge after the spanning-tree state stabilizes.

- CSCdz29910

  While in the interface-range configuration mode, if you use the **no channel-group** interface configuration command or change the channel-group mode by using the **channel-group** command, an assert-fail message with traceback information no longer appears.

- CSCdz41019

  In a switch stack, if the stack master is reloaded at the same time that an EtherChannel link on a stack member goes down, the new stack master no longer fails shortly after being elected.

- CSCdz60348

  When an output ACL for a VLAN is full, the switch no longer drops all the packets routed or sent to that VLAN. This problem no longer occurs for Layer 3 features, such as unicast routing, multicast routing, and fallback bridging.

- CSCdz69741

  If there is a lot of SNMP polling activity and MAC notification traps being sent on the switch, entering the **mac-address-table notification history-size** *value* global configuration command to change the MAC address notification table history size no longer causes the switch to fail.

- CSCdz71127

  See CSCea02355.

- CSCdz79082

  A broadcast storm no longer occurs in a bridge group under these conditions:

  - When a port in the VLAN in which fallback bridging is enabled receives a non-IP packet with the bridge protocol data unit (BPDU) indicator bit set in the ISL header.
  - The destination MAC address has not been learned in the bridge group and at least one port in the VLAN is in the blocking state.

- CSCea02137

  When an undefined aggregate policer is configured in a policy-map, the switch no longer generates the wrong aggregate policer for it.

- CSCea02355 and CSCdz71127

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

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

  This advisory is available at

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

- CSCea02851

  When you are in policy-map class configuration mode and configure an aggregate policer with the **police aggregate** policy-map class configuration command, causing the number of aggregate policers to exceed 63, the aggregate policer is no longer retained in the policy map.

- CSCea21883

  Under some heavy load conditions with bridge groups and SPAN enabled (where the packets are dropped at the port because of flooding), the %SUPQ-4-CPUHB_RECV_STARVE message no longer appears. During this condition, the port output rate is no longer reduced to recover from the condition.

- CSCea35481

  An extended access list with permit or forward actions using Layer 4 information no longer incorrectly forwards fragmented packets. All packets are correctly forwarded now.

- CSCea54285

  You can now set the VTP mode to transparent (3) by using SNMP.

- CSCea67031

  The switch no longer take several minutes to generate and optimize the forwarding rules after you configure a complex VLAN map. For example, a complex VLAN map might contain multiple sequences that use the same VLAN map ACL, where the individual ACL clauses include one or more deny clauses (nonterminating–not the last deny). During the optimization process, the switch now responds to commands.

- CSCea75726

  When snooping is disabled and a spanning tree loop exists, incoming IGMP report and leave messages no longer generate a storm of such messages in the network.

- CSCea86944

  Gigabit Ethernet ports configured for RGMII mode (1/2, 5/6, 9/10, 13/14, 17/18, and 21/22) no longer fail an internal loopback test during system startup on the Catalyst 3750G-24T and Catalyst 3750G-24TS switches.

- CSCea88723

  A routed port that uses an IP ACL no longer filters packets incorrectly after an administrative shutdown and restart. The problem previously occurred after the following sequence:

  – An IP ACL is applied to a routed port by using the **ip access-group** interface configuration command.

  – The routed port is shut down by using the **shutdown** interface configuration command.

  – The ACL is modified or another interface is changed between routed port and switched port by using the **switchport** and **no switchport** interface configuration commands.

  – The routed port is re-enabled by entering the **no shutdown** interface configuration command.

- CSCeb05555

  The RSPAN feature no longer incorrectly spans all local link control packets with a destination MAC address of 0100.0CCC.CCCC on trunk ports that carry the RSPAN VLAN. Therefore, trunk ports carrying the RSPAN VLAN no longer combine control packets from RSPAN source ports with normal local control packets. The following list describes problems that previously occurred with selected protocols:

  – Cisco Discovery Protocol (CDP) could provide incorrect information. For example, CDP could incorrectly list a neighbor switch that is actually a neighbor on the RSPAN source port.

  - Dynamic Trunking Protocol (DTP) could fail to work properly on trunks that are carrying the RSPAN VLAN.
  - Port Aggregration Protocol (PAgP) could fail to work properly on EtherChannels that are carrying the RSPAN VLAN.
  - VLAN Trunking Protocol (VTP) could incorrectly propagate VTP pruning messages on the wrong interface. For example, a pruning message intended for an RSPAN source port could also appear on the trunk port carrying the RSPAN VLAN.
  - Unidirectional Link Detection Protocol (UDLD) and any other protocol that uses 0100.00CC.CCCC as the destination MAC address could not operate properly on trunk ports that carry the RSPAN VLAN.

- CSCeb43979

  On Catalyst 3750 switches, the rate of traffic routed through the default route is no longer reduced by using software routing rather than hardware routing.

- CSCeb48939

  A switch configured for Rapid Spanning-tree (802.1w) no longer sends a Topology Change Notification (TCN) if an interface is reconfigured by using the **spanning-tree portfast** interface configuration command.

Cisco CMS Caveats Resolved in Release 12.1(14)EA1

These CMS caveats were resolved in Release 12.1(14)EA1:

- CSCdz52326

  In the Voice VLAN window, you can now configure a voice VLAN when the VLAN mode is set to dynamic desirable or dynamic auto.

- CSCea01123

  All Simple Network Management Protocol (SNMP) traps are now shown on the SNMP Trap Managers tab. For example, suppose you click the **Administration > SNMP > Trap Managers** tab, create a trap manager, click the vlancreate and vlandelete checkboxes along with other traps, and click **Apply**. When you select the new trap manager entry in the Current Managers list, the vlancreate and vlandelete options are now shown.

- CSCea12761

  In the Topology View, when you right-click a device in an expanded switch stack to display the Device Properties window, the model number of the stack master no longer shows in all switches.

- CSCea13508

  From the Users and Passwords window (**Administration > Users and Passwords**), there is now a provision for enabling or disabling the login for console or vty lines.

- CSCea15587

  Whenever a given VLAN has multiple router ports associated with it, the IGMP Router tab on the IGMP Report window (**Reports > Multicast > IGMP Report**) now shows all router ports on a given VLAN.

- CSCea16267

  When you select the **Device > QoS > Policies** window and try to modify a policy, you no longer receive a null-pointer exception error that prevents you from modifying the policy. The error previously occurred when a policy class had an ACL match statement that was deleted.

- CSCea26106

  You can now create or modify an EtherChannel when the ports in the EtherChannel do not meet the following requirements:

  - Port group members must belong to the same set of VLANs and must be all static-access or all trunk ports. The native VLAN ID, trunk VLANs, and pruning VLANs must be the same for trunk ports.
  - Port monitoring (also known as Switched Port Analyzer [SPAN]), port security, 802.1X should not be enabled on the port.
  - Dynamic-access ports cannot be grouped.

- CSCea80729

  The **Refresh** button of the CMS Inventory Report now updates the System Uptime.

Documentation Updates

These are corrections for the *Catalyst 3750 Switch Software Configuration Guide* and *Catalyst 3750 Switch Command Reference*:

- The command syntax for the **udld** interface configuration command is incorrect in the command reference and the software configuration guide. The correct syntax is **udld port** [**aggressive** | **disable**]; the syntax and usage guidelines incorrectly include the **enable** option. Also, the usage guidelines should use **udld port**, not just **udld**, when referring to this command.
- The command syntax for the **mac address-table static** global configuration command is incorrect in the command reference for this release. The correct syntax is **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*.

These changes will be included in the next version of the documentation.

Related Documentation

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

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 31.

- *Catalyst 3750 Switch Software Configuration Guide* (order number DOC-7815164=)
- *Catalyst 3750 Switch Command Reference* (order number DOC-7815165=)
- *Catalyst 3750 Switch System Message Guide* (order number DOC-7815166=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 3750 Switch Hardware Installation Guide* (order number DOC-7815136=)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (not orderable but available on Cisco.com)

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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

Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/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, 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. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments 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

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com 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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing 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.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, 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 website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

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 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 with the documentation listed in the "Related Documentation" section.