



Release Notes for the Catalyst 2970 Switch Cisco IOS Release 12.1(19)EA1

October 2003

The Cisco IOS Release 12.1(19)EA1 runs on all Catalyst 2970 switches.

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 “[Finding the Software Version and Feature Set](#)” section on page 5.
- If you are upgrading to a new release, refer to the software upgrade filename for the software version.

For the complete list of Catalyst 2970 switch documentation, see the “[Related Documentation](#)” section on page 19.

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 in the Cisco IOS software area.



Note

If you are upgrading a switch running Cisco IOS Release 12.1(11)AX 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 12.

Contents

This information is in the release notes:

- [“System Requirements” section on page 2](#)
- [“Downloading Software” section on page 5](#)
- [“Installation Notes” section on page 7](#)
- [“New Features” section on page 8](#)
- [“Limitations and Restrictions” section on page 9](#)
- [“Important Notes” section on page 12](#)
- [“Open Caveats” section on page 13](#)
- [“Resolved Caveats” section on page 18](#)
- [“Documentation Updates” section on page 18](#)
- [“Related Documentation” section on page 19](#)
- [“Obtaining Technical Assistance” section on page 21](#)

System Requirements

These sections describe the system requirements for this software release:

- [“Hardware Supported” section on page 2](#)
- [“Software Compatibility” section on page 3](#)
- [“Cluster Compatibility” section on page 3](#)

Hardware Supported

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

Table 1 *Supported Hardware*

Switch	Description
Catalyst 2970G-24T	24 10/100/1000 Ethernet ports
Catalyst 2970G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots
SFP modules	1000BASE-T, 1000BASE-SX, 1000BASE-LX, CWDM, and 1000BASE-ZX
Redundant power systems	Cisco RPS 300 Redundant Power System Cisco RPS 675 Redundant Power System

Software Compatibility

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

Windows

This release uses a CMS plug-in (Windows only) that replaces the Java plug-in. You can download the plug-in from this URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/CMS-Plug-In-Win-1-0>:



Note

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

Solaris

Java plug-in 1.4.1_02 is required to run CMS. You can download the Java plug-in and installation instructions from this URL:

<http://www.cisco.com/public/sw-center/lan/java/1.4.1-02.html>

Cluster Compatibility

This section describes how to choose command and standby command switches when a cluster consists of a mixture of Catalyst switches. The command switch must be the same type as the standby command switch.

When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch. If your cluster has Catalyst 2970, Catalyst 3550, Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL switches, the Catalyst 3550 switch (with the latest software release) should be the command switch.

Table 2 lists the cluster capabilities and software versions for the switches. The switches are listed from the highest to lowest end. 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	Member or command switch
Catalyst 3550	12.1(4)EA1 or later	Member or command switch
Catalyst 2970	12.1(11)AX	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

Table 2 *Switch Software and Cluster Capability (continued)*

Switch	Cisco IOS Release	Cluster Capability
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

Table 2 *Switch Software and Cluster Capability (continued)*

Switch	Cisco IOS Release	Cluster Capability
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 in 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 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.



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:

- [“Finding the Software Version and Feature Set” section on page 5](#)
- [“Deciding Which Files to Use” section on page 6](#)
- [“Upgrading a Switch by Using CMS” section on page 6](#)
- [“Upgrading a Switch by Using the CLI” section on page 6](#)
- [“Recovering from a Software Failure” section on page 7](#)



Note

Before downloading software, read this section for important information.

Finding 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 number. 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.

Deciding 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 command-line interface (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 2970 Switches

Filename	Description
c2970-i6l2-tar.121-19.EA1.tar	Cisco IOS image file and CMS files. This image has Layer 2+ features.
c2970-i6k2l2-tar.121-19.EA1.tar	Cisco IOS crypto image file and CMS files. This image has the Kerberos and SSH features.

Upgrading a Switch by Using CMS

You can upgrade switch software by using CMS. From the feature 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 2970 switch by using the CLI. 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 6](#) 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 image, select **Catalyst 2970 software**.

To obtain authorization and to download the crypto software files, select **Catalyst 2970 3DES Cryptographic Software**.
 - Step 3** Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.
 - Step 4** Log into 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 software configuration guide for this release.

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 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/c2970-i612-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

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 (Refer to the *Catalyst 2970 Switch Hardware Installation Guide*.)
- The CLI-based setup program (Refer to the *Catalyst 2970 Switch Hardware Installation Guide*.)
- The Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration (Refer to the *Catalyst 2970 Switch Software Configuration Guide*.)
- Manually assigning an IP address (Refer to the *Catalyst 2970 Switch Software Configuration Guide*.)



Note

If you are upgrading a switch running Cisco IOS Release 12.1(11)AX which 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 12.

New Features

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

- [“New Hardware Features” section on page 8](#)
- [“New Software Features” section on page 8](#)

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)EA1 contains these new features or enhancements:

- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts.
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers.
- Internet Group Management Protocol (IGMP) snooping for IGMP version 3 to limit the flooding of multicast traffic.
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table.
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries).
- Unicast MAC filtering to drop packets with specific source or destination MAC addresses.
- Support for the SSHv2 server application.
- Support for an egress priority queue that must be empty before the other three queues are serviced



Note

In the software documentation, *IP* refers to IP version 4 (IPv4).

- CMS support for these new features:
 - The option to install CMS to 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 (Windows only) that replaces the Java plug-in.



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

You can download the plug-in from this URL:

<http://www.cisco.com/pegi-bin/tablebuild.pl/CMS-Plug-In-Win-1-0>

The CMS plug-in includes a console window that you can use for troubleshooting. For more information see the “[Documentation Updates](#)” section on page 18.

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 *Catalyst 2970 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 sections describe the limitations and restrictions:

- “[Cisco IOS Limitations and Restrictions](#)” section on page 9
- “[Cluster Limitations and Restrictions](#)” section on page 11
- “[CMS Limitations and Restrictions](#)” section on page 11

Cisco IOS Limitations and Restrictions

These limitations apply to Cisco IOS configuration:

- If the number of 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. The workaround is to reduce the number of IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, 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 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. (CSCdz11708)

- The Catalyst 2970 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)
- 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)
- 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)
- 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 lose connectivity. 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 the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console. The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
 - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
 - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

There is no workaround. (CSCec20128)
- For trunk ports or access ports configured with 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command. Valid 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

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, re-open it, and launch CMS again. (CSCds29230)
- If you are printing a Topology view or a 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)
- 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 (CSCdz01037).
- 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)
- Running pop-up blocking software with a browser prevents CMS from loading. The workaround is to disable the pop-up blocking software before launching CMS. (CSCec24615)

Important Notes

These sections describe the important notes related to this software release:

- [“Cisco IOS Notes” section on page 12](#)
- [“CMS Notes” section on page 12](#)

Cisco IOS Notes

These notes apply to Cisco IOS configuration:

- The 802.1X feature in Cisco IOS Release 12.1(19)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.
- The Catalyst 2970 switch does not support switch stacking. However, the **show processes** privileged EXEC command still lists stack-related processes. This occurs because the Catalyst 2970 shares common code with other switches that do support stacking.

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 5.5 and select a URL with a nonstandard port at the end of the address (such as *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 from 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.

- 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 5](#).

Open Caveats

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

- [“Open Cisco IOS Caveats” section on page 13](#)
- [“Open CMS Caveats” section on page 15](#)

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.

- CSCeb35422

On a voice VLAN port with both 802.1X and port security enabled, dynamic secure addresses might not be 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 these conditions:

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

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

There is no workaround.

- CSCeb49472
Although it is visible in the command-line help string, the **source-only-learning** keyword is not supported on the Catalyst 2970 switches. Also, the igmp snooping report-suppression feature does not work.
There is no workaround.
- CSCeb66606
When DHCP snooping is enabled, if the lease time given by the server to the client is infinite, tracebacks are generated.
- CSCeb67510
When both the sharing and shaping weights are enabled on Catalyst 2970 switches, the receiving rates might not follow the shared bandwidth weight if the priority queue is enabled on the egress queue.
The workaround is to use lower values of the shaped and shared weights for queues other than the first queue when the egress priority queue is enabled if shaping in other queues is required.
- CSCeb81842
For an interface, if the voice VLAN and the access VLAN are assigned to different VLANs and the access VLAN enters a suspended state, the IP phones do not work.
The workaround is to reset the access VLAN to the active state.
- CSCec07637
When an ACL that denies packets is configured on an ingress or an egress interface, the CPU usage might be as high as 70% because these packets are forwarded to the CPU to determine if an ICMP-unreachable packet should be generated.
There is no workaround.
- CSCec21040
When a 802.1X enabled port is authenticated with a radius-assigned VLAN, the port is shut down or link is removed, and a traceback message appears.
There is no workaround.
- CSCec21320
After a link is up, a switch sends three EAP-Request/Identity messages to the client. There is a 30-second gap between messages. However, PCs that are running Windows XP or Windows 2000 drop the first message so that the second message that the client receives *appears* to be the first, which is at least 30 seconds after the link is up. Therefore, a user does not see a password window until at least 30 seconds after the link is up.
There is no workaround.
- CSCec22572
If per-user access control lists (ACLs) are downloaded from a RADIUS server after successful 802.1X authentication, disabling 802.1X does not remove the attached per-user ACLS from the interface.
The workaround is to enter the **shutdown** and **no shutdown** interface configuration commands to remove the ACLs.

- CSCec29970

If you change the input priority queue for queue 2 by using the **mls qos srr-queue input priority-queue 2 bandwidth** global configuration command, the configurations that are generated contain an extra input keyword such as **mls qos srr-queue input priority-queue input 2 bandwidth**. This extra keyword causes an error message if the command is saved and the switch is reloaded.

This is the workaround:

1. Copy the **config.text** file to a PC or terminal
2. Edit the **config.text** file and remove the extra **input** keyword.
3. Copy the file back to your switch.
4. Reload the switch.

- CSCec31436

When there are many configured secure and sticky MAC addresses on a port, some addresses might be dropped and removed from the configuration when the switch restarts.

There is no workaround.

- CSCec32453

When you configure a unicast MAC address filter that matches a Windows XP 802.1X client MAC address, the switch sends an authentication succeed EAPOL packet to the client followed by an authentication failure EAPOL packet. The Windows XP 802.1X client continues to reauthenticate itself.

There is no workaround.

- CSCec60076

If BPDU filtering is enabled on a trunk port and BPDUs are received on VLANs on which an STP instance is not running, the BPDUs are dropped.

There is no workaround.

Open CMS Caveats

These are the severity 3 CMS configuration caveats:

- 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 no 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 without a warning message. This applies to all switches running Cisco IOS Release 12.1 or later.

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

- CSCeb23416

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

There is no workaround. Make sure that the configuration values entered 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 without a warning message. This applies to all switches running Cisco IOS Release 12.1 or later.

There is no workaround. Make sure that the configuration values entered are valid for the switch type.
- CSCeb38967

When CMS is operating in read-only mode, an error is reported if Help is opened 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.
- CSCec03397

The settings on the Catalyst 2950 LRE ports cannot be modified by using the Port Settings window in CMS.

There is no workaround.
- CSCec09433

You cannot attach an access control list (ACL) to or remove one from an interface when you are in guide mode.

The workaround is to use expert mode to attach an ACL to or remove one from an interface.
- CSCec08618

When you change the Spanning Tree Protocol (STP) port priority on a switch that is running Cisco IOS Release 12.1(19)EA1 or later, the value must range from 0 to 240 and be in an increment of 16. If you enter a value that is not an increment of 16, the configuration fails, and no error message appears.

The workaround is to enter values from 0 to 240 that are in increments of 16.
- CSCec08662

If UplinkFast is enabled and you enter a value in the Path Cost field in the STP Modify Port Parameters window, 3000 is automatically added to the configured-STP cost value. For example, if the path cost is 10, the actual value is 3010. If you disable UplinkFast, the path-cost value changes to its originally configured value of 10.

There is no workaround.

- CSCec16057
CMS does not recognize the CWDM SFP module on the Catalyst 2940 switches, even though the CWDM SPF module is supported by the switches.
There is no workaround.
- CSCec18805
When you launch the IP Multicast wizard, multicast-enabled devices do not appear in the list of multicast-enabled devices.
There is no workaround. The wizard does not display multicast-enabled devices.
- CSCec24473
When you right-click on a Catalyst 3750 switch in the Front Panel view, these pop-up menu options do not appear:
 - The delete-cluster menu option if the Catalyst 3750 switch is a commander switch.
 - The remove-from cluster option if the Catalyst 3750 switch is a member switch.
 The workarounds are to select these menu options from the feature bar:
 - Select **Cluster > Delete Cluster** to delete a cluster from a command switch.
 - Select **Cluster > Remove from Cluster** to remove a member switch.
- CSCec34831
When you click **Highlight VLAN Port Membership Modes** in the VLAN window of a switch whose front panel is not displayed in Front Panel view, CMS brings the Front Panel view to the foreground, but the Front Panel view of the switch is not displayed and you cannot see the highlighted ports.
Use one of these workarounds:
 - From the Front Panel view cluster tree, check the box beside the switch icon so that the switch's front panel is displayed in Front Panel view. Then click **Highlight VLAN Port Membership Modes** in VLAN window. The switch's front panel is displayed and you can see the highlighted ports.
 - After you click **Highlight VLAN Port Membership Modes** in VLAN window, you should check the box beside the switch icon in the Front Panel view cluster tree. The switch's front panel is displayed and you can see the highlighted ports.
- CSCec45975
When you click **Previous** instead of **Finish** in the **Save Configuration** window, the configuration for the interfaces is not applied to the member devices.
The workaround is to click the **Finish** button to apply the configuration to member devices. If you need to modify the configuration, you need to launch the configuration wizard again.
- CSCec47247
The IGMP Report Window does not list all the entries in the table.
There is no workaround.

Resolved Caveats

These sections describe the caveats that have been resolved in this release.

- [“Cisco IOS Caveats Resolved in Cisco IOS Release 12.1\(19\)EA1” section on page 18](#)
- [“Cisco CMS Caveats Resolved in Cisco IOS Release 12.1\(19\)EA1” section on page 18](#)

Cisco IOS Caveats Resolved in Cisco IOS Release 12.1(19)EA1

These Cisco IOS caveats were resolved in Cisco IOS Release 12.1(19)EA1:

- CSCea75390
Local and Remote SPAN can now be configured at the same time.
- CSCeb54159
If an interface on a Catalyst 2970 switch was mapped to queue-set 2 and you disable and then globally re-enable multilayer QoS, the interface is now mapped to the correct egress queue-set (queue-set 2).

Cisco CMS Caveats Resolved in Cisco IOS Release 12.1(19)EA1

This CMS caveat was resolved in Cisco IOS Release 12.1(19)EA1:

- (CSCdv88724)
If a PC running CMS has low memory and CMS is running continuously for 2 to 3 days, the PC no longer runs out of memory.

Documentation Updates

This section provides updates to the product documentation.

Corrections for the Catalyst 2970 Switch Hardware Installation Guide

- This note will be added to the switch installation chapter in the next revision of the documentation.



Note When using shorter lengths of single-mode fiber cable, you might need to insert an inline optical attenuator in the link to avoid overloading the receiver.

When the fiber-optic cable span is less than 15.43 miles (25 km), you should insert a 5-decibel (dB) or 10-dB inline optical attenuator between the fiber-optic cable plant and the receiving port on the 1000BASE-ZX SFP module at each end of the link.

- The CMS requirements as described in the “Managing the Switch by Using the Cluster Management Suite” chapter are no longer correct. Refer to the “Getting Started with CMS” chapter of the software configuration guide for the latest CMS requirements.

Corrections to the Catalyst 2970 Software Configuration Guide

These are corrections for the “Getting Started with CMS” chapter:

- The CMS plug-in includes a console window that you can use to troubleshoot CMS or to view the CLI commands from CMS.

When CMS is running, press **F2** to display or to hide the CMS console. Press **F3** to display or to hide the CLI commands that CMS is sending.

- The chapter incorrectly states that Java plug-in 1.4.1 is required for Solaris. Java plug-in 1.4.1_02 is required to run CMS on Solaris. You can download it from this URL:

<http://www.cisco.com/public/sw-center/lan/java/1.4.1-02.html>

Related Documentation

These documents provide complete information about the switch and are available from this Cisco.com site:

<http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/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 19.

- *Catalyst 2970 Switch Software Configuration Guide* (order number DOC-7815462=)
- *Catalyst 2970 Switch Command Reference* (order number DOC-7815464=)
- *Catalyst 2970 Switch System Message Guide* (order number DOC-7815465=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 2970 Switch Hardware Installation Guide* (order number DOC-7815469=)
- *Cisco RPS 675 Redundant Power System Hardware Installation Guide* (order number DOC-7815201=)
- *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 annual or quarterly subscriptions through the online Subscription Store:

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

Click Subscriptions & Promotional Materials in the left navigation bar.

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 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, 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 (<http://www.cisco.com/tac>) 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.

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

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.

- 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 general networking, training and certification titles. Both new and experienced user 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/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/index.html>

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at

<http://oss.software.ibm.com/icu4j/>

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

