Release Notes for the Catalyst 2960-C Switch, Cisco IOS Release 12.2(55)EX1 and Later

Revised March 29, 2012

Cisco IOS Release 12.2(55)EX3 runs on all Catalyst 2960-C compact switches. See Table 1 to see the minimum Cisco IOS release required by the different switches.

These release notes include important information about Cisco IOS Release 12.2(55)EX1 and later and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see 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, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 5.

You can download the switch software from this site (registered Cisco.com users with a login password): http://www.cisco.com/cisco/web/download/index.html

The Catalyst 2960-C universal image is a LAN base image that supports most of the features supported by the Catalyst 2960 LAN base image in Cisco IOS Release 12.2(55)SE. These features are described in the Catalyst 2960 and 2960-S software configuration guide and command reference for that release.

Note For additional features and information about Catalyst 2960 and 2960-S features that are not supported, see the "Catalyst 2960-C Features" section on page 2.

For basic configuration and command information, see the configuration guide and command reference for the Catalyst 2960 and 2960-S switches for Cisco IOS Release 12.2(55)SE on Cisco.com: http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

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

Contents

Catalyst 2960-C Features

Unless otherwise indicated, the Catalyst 2960-C switches supports all features that are supported by the Catalyst 2960 LAN base image in Cisco IOS Release 12.2(55)SE, including these applications:

- Smart Install—The switch can operate as a Smart Install client only. See the *Smart Install Configuration Guide* for more information: http://www.cisco.com/en/US/docs/switches/lan/smart_install/release_12.2_55_se/configuration/guide/smart_install3.html
- EnergyWise—The switch supports EnergyWise phase 2. See the *EnergyWise Configuration Guide* at http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html

  and the release notes at: http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/release/notes/OL19810.html

The Catalyst 2960 features are documented in the Catalyst 2960 and 2960-S software configuration guide and command reference. The Catalyst 2960-C has these differences:

- Some Catalyst 2960-C switches support PoE pass-through. See the "PoE Uplinks and PoE Pass-Through Capability" section on page 17.
- Some models of the Catalyst 2960-C switches have an USB mini-Type B optional console port and a USB Type A port, like the Catalyst 2960-S switches. The Catalyst 2960CPD-8TT and 2960CPD-8PT switches have only the USB mini-Type B console port.

  See the section on "Using the Switch USB Ports" for the Catalyst 2960-S switch in the software configuration guide and the **media-type rj45** and **usb** line configuration commands in the command reference.
- The Catalyst 2960-C switches support only the default Switch Database Management (SDM) template.
  - The default template is a different template than either the Catalyst 2960 or Catalyst 2960-S default template.
  - You cannot configure any other SDM template on the Catalyst 2960-C.

  - The switch does not support static routing on SVIs.
  - Catalyst 2960CPD-8PT and 2960CPD-8TT switches do not support IPv6 host or IPv6 Multicast Listener Discovery (MLD) snooping.

  See the "The Catalyst 2960-C SDM Template" section on page 19.

The Catalyst 2960-C also does not support these features that are supported on the Catalyst 2960:

- Connections to redundant power supplies
- ISL trunks
- Cisco Express Forwarding
- TCAM consistency check

System Requirements

Supported Hardware

Table 1 Catalyst 2960-C Switches Supported

Switch	Description	Minimum Cisco IOS Release Required
Catalyst 2960CPD-8PT-L	2 10/100/1000 uplink PoE[1]+ input ports to power the switch 8 10/100 PoE ports with PoE pass-through LAN-Base image	Cisco IOS Release 12.2(55)EX1
Catalyst 2960CPD-8TT-L	2 10/100/1000 uplink PoE+ input ports to power the switch 8 10/100 Ethernet ports LAN-Base image	Cisco IOS Release 12.2(55)EX1
Catalyst 2960CG-8TC-L	2 dual-purpose uplink ports (each dual-purpose port has 1 10/100/1000BASE-T copper port and 1 SFP[2] module slot) 8 10/100/1000 Ethernet ports LAN-Base image	Cisco IOS Release 12.2(55)EX1
Catalyst 2960C-8TC-S	2 dual-purpose uplink ports 8 10/100 Ethernet ports LAN-Lite image	Cisco IOS Release 12.2(55)EX3
Catalyst 2960C-8TC-L	2 dual-purpose uplink ports 8 10/100 Ethernet ports LAN-Base image	Cisco IOS Release 12.2(55)EX3

Table 1 Catalyst 2960-C Switches Supported (continued)

Switch	Description	Minimum Cisco IOS Release Required
Catalyst 2960C-8PC-L	2 dual-purpose uplink ports 8 10/100 PoE ports LAN-Base image	Cisco IOS Release 12.2(55)EX3
Catalyst 2960C-12PC-L	2 dual-purpose uplink ports 12 10/100 PoE ports LAN-Base image	Cisco IOS Release 12.2(55)EX3

1. PoE = Power over Ethernet
2. SFP = small form-factor pluggable

Table 2 Other Supported Hardware

Switch	Description	Supported by Minimum Cisco IOS Release
SFP[1] modules	100BASE-BX, FX, -LX 1000BASE-CWDM[2] 100BASE-SX MMF[3] and 100BASE-SX, -H SMF[4] For complete lists of supported SFP modules, see the hardware installation guide and the documents on this page: http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html	Cisco IOS Release 12.2(55)EX1

1. SFP = Small-form pluggable.
2. CWDM = coarse wavelength-division multiplexer.
3. MMF = multimode fiber.
4. SMF = single-mode fiber.

Device Manager System Requirements

Hardware Requirements

Table 3 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software Requirements

- Windows 2000, XP, Vista, and Windows Server 2003.

- Internet Explorer 6.0 or 7.0, and Firefox up to version 27, with JavaScript enabled.

Device Manager verifies the browser version when starting a session and does not require a plug-in.

Upgrading the Switch Software

- Finding the Software Version and Feature Set, page 5
- Deciding Which Files to Use, page 5
- Archiving Software Images, page 5
- Upgrading a Switch by Using the Device Manager, page 6
- Upgrading a Switch by Using the CLI, page 6
- Recovering from a Software Failure, page 7

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. 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 of the display shows the version.

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.

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 the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the CLI, use the tar file and the **archive download-sw** privileged EXEC command.

Table 4 Cisco IOS Software Image Files

Filename	Description
c2960c-universalk9-tar.122-55.EX3.tar	Catalyst 2960-C LAN base and LAN Lite cryptographic image file and device manager files. This image has the Kerberos and SSH features.

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*:
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using the Device Manager

You can upgrade switch software by using the device manager. For detailed instructions, click **Help**.

Note When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the 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, follow these steps:

Step 1 Use Table 4 on page 5 to identify the file that you want to download.

Step 2 Download the software image file:

a. If you are a registered customer, go to this URL and log in.

http://www.cisco.com/cisco/web/download/index.html

b. Navigate to **Switches** > **LAN Switches - Access**.

c. Navigate to your switch model.

d. Click **IOS Software** and select the latest Cisco IOS release.

Download the image that you identified in Step 1.

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, see 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 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

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

For more information about assigning an IP address and default gateway to the switch, see 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 software version that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# 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/c2960c-universalk9-tar.122-55.EX3.tar
```

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

Recovering from a Software Failure

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

Installation Notes

Use these methods to assign IP information to your switch:

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the 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.

- Cisco IOS Limitations, page 8
- Device Manager Limitations, page 13

Cisco IOS Limitations

- Configuration, page 8
- Ethernet, page 9
- IP Telephony, page 10
- Multicasting, page 10
- Power, page 11
- QoS, page 11
- RADIUS, page 11
- Smart Install, page 12
- SPAN and RSPAN, page 12
- Trunking, page 12
- VLAN, page 12

Configuration

- 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 up without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give it an address (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 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)
- A traceback error occurs if a crypto key is generated after an SSL client session.

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)
- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).
- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a nonzero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)
- A ciscoFlashMIBTrap message appears during switch startup. This does not affect switch functionality. (CSCsj46992)

Ethernet

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

  If this happens, uneven traffic distribution occurs on EtherChannel ports.

  Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem. Use any of these workarounds to improve EtherChannel load balancing:

  - for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
  - for incrementing source-ip traffic, configure load balance method as **src-ip**
  - for incrementing dest-ip traffic, configure load balance method as **dst-ip**
  - Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

  For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

IP Telephony

- After you change the access VLAN on a port that has IEEE 802.1x enabled, the IP phone address is removed. Because learning is restricted on IEEE 802.1x-capable ports, it takes approximately 30 seconds before the address is relearned. No workaround is necessary. (CSCea85312)
- Some access point devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These access points should be discovered as Cisco prestandard devices. The **show power inline** user EXEC command shows the access point as an IEEE Class 1 device. The workaround is to power the access point by using an AC wall adaptor. (CSCin69533)
- The Cisco 7905 IP Phone is error-disabled when the phone is connected to wall power.

  The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

Multicasting

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by 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)
- 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)
- If an IG MP 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)
- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

  The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

  There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

  After you configure a switch to join a multicast group by entering the **ip igmp join-group** *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

  Use one of these workarounds:
  - Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
  - Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)

Power

- Entering the **shutdown** and the **no shutdown** interface configuration commands on the internal link can disrupt the PoE operation. If a new IP phone is added while the internal link is in shutdown state, the IP phone does not get inline power if the internal link is brought up within 5 minutes.

  The workaround is to enter the **shutdown** and the **no shutdown** interface configuration commands on the Fast Ethernet interface of a new IP phone that is attached to the service module port after the internal link is brought up. (CSCeh45465)

QoS

- 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)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different. There is no workaround. (CSCee22591)
- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

  ```
  01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
  ```

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

RADIUS

- RADIUS change of authorization (COA) reauthorization is not supported on the critical auth VLAN.

  There is no workaround. (CSCta05071)

Smart Install

- If the director in the Smart Install network is between an access point and the DHCP server, the access point tries to use the Smart Install feature upgrade, even though access points are not supported devices. The upgrade fails because the director does not have an image and a configuration file for the access point.

  There is no workaround. (CSCtg98656)

SPAN and RSPAN

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session. The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface.

  There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is 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).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 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).

VLAN

- 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)
- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port. (CSCsi26392)

Device Manager Limitations

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

  The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Important Notes

- Cisco IOS Notes, page 13
- Device Manager Notes, page 13

Cisco IOS Notes

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, check that there is network connectivity between the switch and the ACS. You should also check that the switch has been properly configured as an AAA client on the ACS

Device Manager Notes

- Although visible in the Device Manager online help graphic, the USB Type A port is not supported on the Catalyst 2960CPD-8PT-L and the 2960CPD-8TT-L switches.
- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager sessions on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.
- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer:
  1. Choose **Tools** > **Internet Options**.
  2. Click **Settings** in the “Temporary Internet files” area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

  If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface authentication method:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used. • **tacacs**—TACACS server is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

Open Caveats

- CSCte99366

  In a Smart Install network, when the director is connected between the client and the DHCP server and the server has options configured for image and configuration, the client does not receive the image and configuration files sent by the DHCP server during an automatic upgrade. Instead, the files are overwritten by the director, and the client receives the image and configuration that the director sends.

  Use one of these workarounds:

  - If client needs to upgrade by using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.
  - In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director.

- CSCtn63840

  When you add a static EnergyWise neighbor to a Catalyst 2960-C switch, a traceback error could occur or the switch could reload under these circumstances:

  - The Catalyst 2960-C switch is connected to a Catalyst 3750G switch
  - The Catalyst 3750G switch is acting as a router and does not have EnergyWise enabled
  - The Catalyst 3750G switch is connected to a third switch that has EnergyWise enabled and a PoE device attached

  The problem can occur when you enter the **energywise neighbo**r [*hostname* | *ip-address*] *udp-port-number* global configuration command on the Catalyst 2960-C to try to add the third switch as an EnergyWise neighbor.

  The workaround is to establish the route by pinging the EnergyWise switch before you enter the **energywise neighbor** command.

- CSCtg71149

  When ports in an EtherChannel are linking up, the message `EC-5-CANNOT_BUNDLE2` might appear. This condition is often self-correcting, shown by the appearance of an `EC-5-COMPATIBLE` message following the first message. On occasion, the issue does not self-correct, and the ports might remain unbundled.

  The workaround is to reload the switch or to restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order:

  - Enter the **shutdown** interface configuration command on each member port.
  - Enter the **shutdown** command on the port-channel interface.
  - Enter the **no shutdown** command on each member port.
  - Enter the **no shutdown** command on the port-channel interface.

- CSCtq87110

  On a WS-C2960CG-8TC-L switch, if you use the manual bootloader to boot up the software using the *switch:* prompt, the console port LED might not light to indicate whether the RJ-45 or mini-USB console is being used for output. When the switch is set to auto-boot Cisco IOS, the LEDs operate correctly. The problem is visible only when you stop the auto-boot process to access the bootloader.

  There is no workaround.

- CSCtu00997

  Although you can apply the LAN base routing template to the switch, you cannot use the **ip routing** global configuration command.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 12.2(55)EX3

- CSCto10165

  A vulnerability exists in the Smart Install feature of Cisco Catalyst Switches running Cisco IOS Software that could allow an unauthenticated, remote attacker to perform remote code execution on the affected device.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available to mitigate this vulnerability other than disabling the Smart Install feature.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-smart-install.shtml.

- CSCtn63840

  When you add a static EnergyWise neighbor to a Catalyst 2960-C switch, a traceback error could occur or the switch could reload under these circumstances:

  - The Catalyst 2960-C switch is connected to a Catalyst 3750G switch
  - The Catalyst 3750G switch is acting as a router and does not have EnergyWise enabled
  - The Catalyst 3750G switch is connected to a third switch that has EnergyWise enabled and a PoE device attached

  The problem can occur when you enter the **energywise neighbo**r [*hostname* | *ip-address*] *udp-port-number* global configuration command on the Catalyst 2960-C to try to add the third switch as an EnergyWise neighbor.

  The workaround is to establish the route by pinging the EnergyWise switch before you enter the **energywise neighbor** command.

Documentation Updates

- Updates to the Catalyst 3560-C and 2960-C Switch Hardware Documentation, page 17
- Updates to the Catalyst 2960 Switch Software Configuration Guide, page 17
- Updates to the Catalyst 2960 Switch Command Reference, page 20
- Updates to the Catalyst 2960 System Message Guide, page 34

Updates to the Catalyst 3560-C and 2960-C Switch Hardware Documentation

- Network Assistant supported only on these switches:

  Catalyst 2960CG-8TC-L, 2960CPD-8PT-L, and 2960CPD-8TT-L
- Update to the "Rear Panel" section in the "Overview Chapter" of the hardware guide:

  The heat sink fins are present on the Catalyst 3560CG-8PC-S, 2960C-8PC-L, 2960C-12PC-L 3560C-8PC-S, and 3560C-12PC-S switches.

Updates to the Catalyst 2960 Switch Software Configuration Guide

- PoE Uplinks and PoE Pass-Through Capability, page 17
- The Catalyst 2960-C SDM Template, page 19

PoE Uplinks and PoE Pass-Through Capability

The Catalyst 2960-C compact switches can receive power on the two uplink Gigabit Ethernet ports from a PoE or PoE+ capable-switch (for example a Catalyst 3750-X or 3560-X switch). The switch can also receive power from an AC power source when you use the auxiliary power input. When both uplink ports and auxiliary power are connected, the auxiliary power input takes precedence.

The Catalyst 2960CPD-8PT switch can provide power to end devices through the eight downlink ports in one of two ways:

- When the switch receives power from the auxiliary power input, it acts like any other PoE switch and can supply power to end devices connected to the eight downlink ports according to the total power budget. Possible end devices are IP phones, video cameras, and access points.
- When the switch receives power through one or both uplink ports, it can provide PoE pass-through, taking the surplus power from the PoE or PoE+ uplinks and passing it through the downlink ports to end devices. The available power depends on the power drawn from the uplink ports and varies, depending if one or both uplink ports are connected and if the source is PoE or PoE+.

The downlink ports are PoE-capable, and each port can supply up to 15.4 W per port to a connected powered device. When the switch draws power from the uplink ports, the power budget (the available power on downlink ports) depends on the power source options shown in Table 5. When the switch receives power through the auxiliary connector, the power budget is similar to that of any other PoE switch.

Table 5 Catalyst 2960CPD-8PT Power Budget

Power Source Options	Power Sent from Uplink Switches	Available PoE Budget
1 PoE uplink port	15.4 W	0
2 PoE uplink ports	30.8 W	7 W
1 PoE+ uplink port	30 W	7 W
1 PoE and 1 PoE+ uplink	45.4 W	15.4 W
2 PoE+ uplink ports	60 W	22.4 W
Auxiliary power input	—	22.4 W

You can configure the power management, budgeting, and policing the same as with any other Catalyst 2960 or 2960-S PoE switch. See the configuration information starting with the "Configuring Power Management Mode on a PoE Port" section in the *Catalyst 2960 and 2960-S Software Configuration Guide*.

The **show env power inline** privileged EXEC command provides information about powering options and power backup on your switch:

```
Switch# show env power
PoE Power - Available:22.4(w)  Backup:0.0(w)

Power Source   Type           Power(w)  Mode
-------------- -------------- --------- ---------
A.C. Input     Auxilliary     51(w)     Available
Gi0/2          Type1          15.4(w)   Back-up

Available : The PoE received on this link is used for powering this switch and
            providing PoE pass-through if applicable.
Back-up   : In the absence of 'Available' power mode, the PoE received on this
            link is used for powering this switch and providing PoE pass-through
           if applicable.
Available*: The PoE received on this link is used for powering this switch but
            does not contribute to the PoE pass-through.
Back-up*  : In the absence of 'Available' power mode, the PoE received on this
            link is used for powering this switch but does not contribute to
            the PoE pass-through.
```

You can see the available power and the power required by each connected device by entering the **show power inline** privileged EXEC command. This is an example of output from a Catalyst 2960CPD-8PT:

```
Switch# show power inline
Available:22.4(w)  Used:15.4(w)  Remaining:7.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   off        0.0     n/a                 n/a   15.4
Fa0/2     auto   off        0.0     n/a                 n/a   15.4
Fa0/3     auto   off        0.0     n/a                 n/a   15.4
Fa0/4     auto   off        0.0     n/a                 n/a   15.4
Fa0/5     auto   on         15.4    IP Phone 8961       4     15.4
Fa0/6     auto   off        0.0     n/a                 n/a   15.4
Fa0/7     auto   off        0.0     n/a                 n/a   15.4
Fa0/8     auto   off        0.0     n/a                 n/a   15.4
```

Enter the **show power inline police** privileged EXEC command to see power monitoring status. This is an example of output from a Catalyst 2960CPD-8PT:

```
Switch# show power inline police
Available:22.4(w)  Used:15.4(w)  Remaining:7.0(w)

Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Fa0/1     auto   off        none       n/a        n/a    0.0
Fa0/2     auto   off        none       n/a        n/a    0.0
Fa0/3     auto   off        none       n/a        n/a    0.0
Fa0/4     auto   off        none       n/a        n/a    0.0
Fa0/5     auto   on         none       n/a        n/a    9.5
Fa0/6     auto   off        none       n/a        n/a    0.0
Fa0/7     auto   off        none       n/a        n/a    0.0
Fa0/8     auto   off        none       n/a        n/a    0.0
--------- ------ ---------- ---------- ---------- ------ -----
Totals:                                                  9.5
```

The Catalyst 2960CPD-8TT and Catalyst 2960CG-8TC downlink ports cannot provide power to end devices. This is an example of output from the **show power inline** command on a C2960CPD-8TT switch:

```
Switch# show power inline
Available:0.0(w)  Used:0.0(w)  Remaining:0.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
```

The **show power inline dynamic-priority** command shows the power priority of each port:

```
Switch# show power inline dynamic-priority
 Dynamic Port Priority
-----------------------
Port      OperState Priority
--------- --------- --------
Fa0/1     off       High
Fa0/2     off       High
Fa0/3     off       High
Fa0/4     off       High
Fa0/5     off       High
Fa0/6     off       High
Fa0/7     off       High
Fa0/8     off       High
```

The Catalyst 2960-C SDM Template

The Catalyst 2960-C Gigabit Ethernet switch supports only the SDM default template, which is different from the Catalyst 2960 or Catalyst 2960-S default template. Because of the compact size of the switch, memory capacity is less, which can result in reduced support for a feature, for example, allowing fewer MAC addresses. All Catalyst 2960-C default templates support 0 routed interfaces and 255 VLANs.

On the Catalyst 2960C Gigabit Ethernet switches, the default template includes support for IPv6 features. On the Catalyst 2960CPD-8PT and 2960CPD-8TT Fast Ethernet switches, the default template does not include support for IPv6 features and IPv6 features. IPv6 host functions or IPv6 MLD snooping, are not supported for this release.

Table 6 Approximate Resource Allocation by Catalyst 2960-C Default Templates

Resource	Catalyst 2960CG-8TC Gigabit Ethernet switch	Catalyst 2960CPD-8PT and 2960CPD-8TT Fast Ethernet Switches
Unicast MAC addresses	8 K	8 K
IPv4 IGMP groups	0.25 K	0.25 K
IPv6 multicast groups	0.25 K	0
IPv4 MAC/QoS classification ACEs	0.125 K	0.125 K
IPv4 MAC/Security ACEs	0.375 K	0.375 K
IPv6 policy based routing ACEs	0	0
IPv6 QoS ACEs	60	0
IPv6 security ACEs	0.125 K	0

Because the Catalyst 2960-C Gigabit Ethernet switch supports only the default template, entering the **sdm prefer** global configuration command has no effect.

Starting with Cisco IOS Release 12.2(55)EX3, Catalyst 2960-C Fast Ethernet switches support multiple templates: default, dual IPv4 and IP v6, and QoS. All Catalyst 2960-C templates support 0 routed interfaces and 255 VLANs.

See the sdm prefer and show sdm prefer commands in the next section for details on the features supported.

Updates to the Catalyst 2960 Switch Command Reference

These commands are new or modified:

- auto qos video, page 21 (document update not specific to the Catalyst 2960-C switch)
- sdm prefer, page 24
- show power inline, page 28
- show sdm prefer, page 32

auto qos video

Use the **auto qos video** interface configuration command on the switch stack or on a standalone switch to automatically configure quality of service (QoS) for video within a QoS domain. Use the **no** form of this command to return to the default setting.

auto qos video {**cts** | **ip-camera**}

no auto qos video {**cts** | **ip-camera**}

Syntax Description

cts	Identify this port as connected to a Cisco TelePresence System and automatically configure QoS for video.
ip-camera	Identify this port as connected to a Cisco IP camera and automatically configure QoS for video.

Defaults

Auto-QoS video is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Table 7 Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP[1] BPDU[2] Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP[3]	46	24, 26	48	56	34	–	
CoS[4]	5	3	6	7	3	–	
CoS-to-ingress queue map	4, 5 (queue 2)					0, 1, 2, 3, 6, 7 (queue 1)	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)			0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

[1] STP = Spanning Tree Protocol.

[2] BPDU = bridge protocol data unit.

[3] DSCP = Differentiated Services Code Point.

[4] CoS = class of service.

Table 8 Auto-QoS Configuration for the Ingress Queues

Ingress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size
SRR[1] shared	1	0, 1, 2, 3, 6, 7	70 percent	90 percent
Priority	2	4, 5	30 percent	10 percent

[1] SRR = shaped round robin. Ingress queues support shared mode only.

Table 9 Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

Command Modes

Interface configuration

Command History

Release	Modification
12.2(55)SE	This command was introduced.

Usage Guidelines

Use this command to configure the QoS appropriate for video traffic within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-Qos configures the switch for video connectivity with a Cisco TelePresence system and a Cisco IP camera.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

Note The switch applies the auto-QoS-generated commands as if the commands were entered from the CLI. An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands are not applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enable the auto-QoS feature on the first port, these automatic actions occur:

- QoS is globally enabled (**mls qos** global configuration command), and other global configuration commands are added.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging. For more information, see the **debug auto qos** command.

To disable auto-QoS on a port, use the **no auto qos video** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos video** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration). You can use the **no mls qos** global configuration command to disable the auto-QoS-generated global configuration commands. With QoS disabled, there is no concept of trusted or untrusted ports because the packets are not modified (the CoS, DSCP, and IP precedence values in the packet are not changed). Traffic is switched in pass-through mode (packets are switched without any rewrites and classified as best effort without any policing).

Examples

This example shows how to enable auto-QoS for a Cisco Telepresence interface with conditional trust. The interface is trusted only if a Cisco Telepresence device is detected; otherwise, the port is untrusted.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos video cts
```

You can verify your settings by entering the **show auto qos video interface** *interface-id* privileged EXEC command.

Related Commands

Command	Description
debug auto qos	Enables debugging of the auto-QoS feature.
mls qos trust	Configures the port trust state.
srr-queue bandwidth share	Assigns the shared weights and enables bandwidth sharing on the four egress queues mapped to a port.
queue-set	Maps a port to a queue-set.
show auto qos	Displays auto-QoS information.
show mls qos interface	Displays QoS information at the port level.

sdm prefer

Use the **sdm prefer** global configuration command to configure the template used in Switch Database Management (SDM) resource allocation. You can use a template to allocate system resources to best support the features being used in your application. Use the **no** form of this command to return to the default template.

For Catalyst 2960 switches:

sdm prefer {**default** | **dual-ipv4-and-ipv6 default** | **lanbase-routing** | **qos**}

no sdm prefer

For Catalyst 2960-C Fast Ethernet switches:

sdm prefer {**default** | **dual-ipv4-and-ipv6 default** | **qos**}

no sdm prefer

For Catalyst 2960-S switches:

sdm prefer {**default** | **lanbase-routing**}

no sdm prefer

For Catalyst 2960-C Gigabit Ethernet switches:

sdm prefer default

Syntax Description

default	Give balance to all functions. **Note** This is the only template supported on the Catalyst 2960-C switch.
dual-ipv4-and-ipv6 default	Allows the switch to be used in dual stack environments (supporting both IPv4 and IPv6 forwarding). On Catalyst 2960 switches running the LAN base image, you configure this template to enable IPv6 MLD snooping or IPv6 host functions (not required on Catalyst 2960-S or 2960-C switches).
lanbase-routing	Supports configuring 16 IPv4 static unicast routes on switch virtual interfaces (SVIs). This template is available only on Catalyst 2960 or 2960-S switches running the LAN base image.
qos	Provide maximum system usage for quality of service (QoS) access control entries (ACEs). This template is not required on Catalyst 2960-C or 2960-S switches.

Defaults

The **default** template provides a balance to all features.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)FX	This command was introduced.
12.2(40)SE	The **dual-ipv4-and-ipv6 default** keywords were added.
12.2(55)SE	The **lanbase-routing** keyword was added to switches running the LAN base image.
12.2(55)EX	The Catalyst 2960-C templates were added.

Usage Guidelines

You must reload the switch for the configuration to take effect.

If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

Use the **no sdm prefer** command to set the switch to the default template.

Template resources are based on 0 routed interfaces and 255 VLANs, except for the LAN base routing template, which supports 8 routed interfaces and 255 VLANs.

A Catalyst 2960-S switch running the LAN base image uses a default template that includes maximum resources for all supported features; it does not require the dual or qos templates. However, to enable static routing on the Catalyst 2960-S switch, you must configure the lanbase-routing template.

Catalyst 2960-C Gigabit Ethernet switches support only a default template.

For Catalyst 2960 switches and Catalyst 2960-C Fast Ethernet switches:

- Do not use the ipv4-and-ipv6 template if you do not plan to enable IPv6 functionality on the switch. Entering the **sdm prefer ipv4-and-ipv6** global configuration command divides resources between IPv4 and IPv6, which limits those allocated to IPv4 forwarding.

For Catalyst 2960 switches:

- Do not use the routing template if you are not using static routing on your switch. Entering the **sdm prefer lanbase-routing** global configuration command prevents other features from using the memory allocated to unicast routing in the routing template.

Enter the **show sdm prefer** privileged EXEC command to see which template is active on the switch or to see the resource allocations of any template.

Table 10 Approximate Feature Resources Allowed on Catalyst 2960 Switch Templates

Resource	Default	QoS	Dual	LAN base routing
Unicast MAC addresses	8 K	8 K	8 K	4 K
IPv4 IGMP groups	256	256	256	256
IPv4 unicast routes	0	0	0	.75 K
• Directly connected hosts	0	0	0	.75 K
• Indirect routes	0	0	0	16
IPv6 multicast groups	0	0	0	0
Directly connected IPv6 addresses	0	0	0	0
Indirect IPv6 unicast routes	0	0	0	0

Table 10 Approximate Feature Resources Allowed on Catalyst 2960 Switch Templates (continued)

Resource	Default	QoS	Dual	LAN base routing
IPv4 policy-based routing aces	0	0	0	0
IPv4 MAC QoS ACEs	128	384	0	128
IPv4 MAC security ACEs	384	128	256	384
IPv6 policy-based routing aces	0	0	0	0
IPv6 QoS ACEs	0	0	0	0
IPv6 security ACEs	0	0	0	0

Table 11 Approximate Feature Resources Allowed on 2960-S Switch Templates

Resource	Default	LAN base routing
Unicast MAC addresses	8K	4 K
IPv4 IGMP groups	256	256
IPv4 unicast routes	256	.75 K
• Directly connected hosts		.75 K
• Indirect routes		16
IPv6 multicast groups		0
Directly connected IPv6 addresses		0
Indirect IPv6 unicast routes		0
IPv4 policy-based routing aces		0
IPv4 MAC QoS ACEs	384	128
IPv4 MAC security ACEs	384	384
IPv6 policy-based routing aces		0
IPv6 QoS ACEs		0
IPv6 security ACEs	128	0

Table 12 Approximate Feature Resources Allowed on 2960-C Gigabit Ethernet Switch Templates

Resource	Default
Unicast MAC addresses	8K
IPv4 IGMP groups	.25 K
IPv6 multicast groups	.25 K
Directly connected IPv6 addresses	
Indirect IPv6 unicast routes	
IPv4 policy-based routing aces	
IPv4 MAC QoS ACEs	.125 K
IPv4 MAC security ACEs	.375 K
IPv6 policy-based routing aces	0
IPv6 QoS ACEs	60
IPv6 security ACEs	.125

Table 13 Approximate Feature Resources Allowed on Catalyst 2960-C Fast Ethernet Switch Templates

Resource	Default	QoS	Dual
Unicast MAC addresses	8 K	8 K	8 K
IPv4 IGMP groups and multicast routes	.25 K	.25 K	.25 K
IPv4 unicast routes	0	0	0
• Directly connected hosts	0	0	0
• Indirect routes	0	0	0
IPv6 multicast groups	0	0	.375 K
Directly connected IPv6 addresses	0	0	0
Indirect IPv6 unicast routes	0	0	0
IPv4 policy-based routing aces	0	0	0
IPv4 MAC QoS ACEs	.125 K	.375 K	.125 K
IPv4 MAC security ACEs	.375 K	.125 K	.375 K
IPv6 policy-based routing aces	0	0	0
IPv6 QoS ACEs	0	0	20
IPv6 security ACEs	0	0	77

Examples

This example shows how to use the QoS template:

```
Switch(config)# sdm prefer qos
Switch(config)# exit
Switch# reload
```

This example shows how to configure the dual IPv4-and-IPv6 default template on a switch:

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default
Switch(config)# exit
Switch# reload
```

This example shows how to configure the default template on a switch:

```
Switch(config)# sdm prefer default
Switch(config)# exit
Switch# reload
```

Related Commands

Command	Description
show sdm prefer	Displays the current SDM template in use or displays the templates that can be used, with approximate resource allocation per feature.

show power inline

Use the **show power inline** user EXEC command to display the Power over Ethernet (PoE) status for the specified PoE port or for all PoE ports.

show power inline [**police** [*interface-id*] | **consumption** | **dynamic-priority**]

Syntax Description

police	(Optional) Display the power policing information about real-time power consumption.
interface-id	(Optional) Display PoE-related power management information for the specified interface.
consumption	(Optional) Display the power allocated to devices connected to PoE ports.
dynamic-priority	(Optional) Display the dynamic priority of each PoE interface. This keyword is supported only on Catalyst 2960-C switches.

Command Modes

User EXEC

Command History

Release	Modification
12.2(55)EX1	The **dynamic-priority** keyword was added.

Examples

This is an example of output from the **show power inline** command on a Catalyst 2960CPD-8PT: It shows the available power and the power required by each connected device by entering

```
Switch# show power inline
Available:22.4(w)  Used:15.4(w)  Remaining:7.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   off        0.0     n/a                 n/a   15.4
```

```
Fa0/2     auto   off        0.0     n/a                 n/a   15.4
Fa0/3     auto   off        0.0     n/a                 n/a   15.4
Fa0/4     auto   off        0.0     n/a                 n/a   15.4
Fa0/5     auto   on         15.4    IP Phone 8961       4     15.4
Fa0/6     auto   off        0.0     n/a                 n/a   15.4
Fa0/7     auto   off        0.0     n/a                 n/a   15.4
Fa0/8     auto   off        0.0     n/a                 n/a   15.4
```

Table 14 describes the output fields.

Table 14 show power inline Field Descriptions

Field	Description
Admin	Administration mode: auto, off, static
Oper	Operating mode: - on—the powered device is detected, and power is applied. - off—no PoE is applied. - faulty—device detection or a powered device is in a faulty state. - power-deny—a powered device is detected, but no PoE is available, or the maximum wattage exceeds the detected powered-device maximum.
Power	The supplied PoE in watts
Device	The device type detected: n/a, unknown, Cisco powered-device, IEEE powered-device, <name from CDP>
Class	The IEEE classification: n/a, Class <0–4>
Max	The maximum power for each device.

The Catalyst 2960CPD-8TT and Catalyst 2960CG-8TC downlink ports cannot provide power to end devices. This is an example of output from the **show power inline** command on a Catalyst 2960CPD-8TT switch:

```
Switch# show power inline
Available:0.0(w)  Used:0.0(w)  Remaining:0.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
```

This is an example of the output of the **show power inline police** privileged EXEC command on a Catalyst 2960CPD-8PT:

```
Switch# show power inline police
Available:22.4(w)  Used:15.4(w)  Remaining:7.0(w)

Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Fa0/1     auto   off        none       n/a        n/a    0.0
Fa0/2     auto   off        none       n/a        n/a    0.0
Fa0/3     auto   off        none       n/a        n/a    0.0
Fa0/4     auto   off        none       n/a        n/a    0.0
Fa0/5     auto   on         none       n/a        n/a    9.5
Fa0/6     auto   off        none       n/a        n/a    0.0
Fa0/7     auto   off        none       n/a        n/a    0.0
Fa0/8     auto   off        none       n/a        n/a    0.0
--------- ------ ---------- ---------- ---------- ------ -----
```

```
Totals:                                             9.5
```

Table 15 describes the output fields.

Table 15 show power inline police Field Descriptions

Field	Description
Interface	Interface connected to a PoE device.
Admin State	Administration mode: auto, off, static.
Oper State	Operating mode: • errdisable—Policing is enabled. • faulty—Device detection on a powered device is in a faulty state. • off—No PoE is applied. • on—The powered device is detected, and power is applied. • power-deny—A powered device is detected, but no PoE is available, or the real-time power consumption exceeds the maximum power allocation. **Note** The operating mode is the current PoE state for the specified PoE port or for all PoE ports on the switch.
Admin Police	Status of the real-time power-consumption policing feature: • errdisable—Policing is enabled, and the switch shuts down the port when the real-time power consumption exceeds the maximum power allocation. • log—Policing is enabled, and the switch generates a syslog message when the real-time power consumption exceeds the maximum power allocation. • none—Policing is disabled.
Oper Police	Policing status: • errdisable—The real-time power consumption exceeds the maximum power allocation, and the switch shuts down the PoE port. • log—The real-time power consumption exceeds the maximum power allocation, and the switch generates a syslog message. • n/a—Device detection is disabled, power is not applied to the PoE port, or no policing action is configured. • ok—Real-time power consumption is less than the maximum power allocation.
Cutoff Power	The maximum power allocated on the port. When the real-time power consumption is greater than this value, the switch takes the configured policing action.
Oper Power	The real-time power consumption of the powered device.

This is an example of output from the **show power inline police** *interface-id* command on a switch.

```
Switch> show power inline police gigabitethernet0/4
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi0/4     auto   power-deny log        n/a        4.0    0.0
```

This is an example of output from the **show power inline consumption** command on all PoE switch ports:

```
Switch> show power inline consumption
Default PD consumption : 15400 mW
```

This is an example of output from the **show power inline dynamic-priority** command on a switch.

```
Switch> show power inline dynamic-priority
Dynamic Port Priority
-----------------------
Port      OperState Priority
--------- --------- --------
Fa0/1     off       High
Fa0/2     off       High
Fa0/3     off       High
Fa0/4     off       High
Fa0/5     off       High
Fa0/6     off       High
Fa0/7     off       High
Fa0/8     off       High
```

Related Commands

Command	Description
logging event power-inline-status	Enables the logging of PoE events.
power inline	Configures the power management mode for the specified PoE port or for all PoE ports.
show controllers power inline	Displays the values in the registers of the specified PoE controller.

show sdm prefer

Use the **show sdm prefer** privileged EXEC command to display information about the Switch Database Management (SDM) template used for allocating system resources for a particular feature.

For Catalyst 2960 switches:

show sdm prefer [**default** | **dual-ipv4-and-ipv6 default** | **lanbase-routing** | **qos**]

For Catalyst 960-C Fast Ethernet switches:

show sdm prefer [**default** | **dual-ipv4-and-ipv6 default** | **qos**]

For Catalyst 2960-S switches:

show sdm prefer [**default** | **lanbase-routing**]

For Catalyst 2960-C Gigabit Ethernet switches:

show sdm prefer default

Syntax Description

default	(Optional) Display the template that balances system resources among features. This is the only template supported on Catalyst 2960-S and Catalyst 2960-C Gigabit Ethernet switches.
dual-ipv4-and-ipv6 default	(Optional) Display the dual template that supports both IPv4 and IPv6.
lanbase-routing	(Optional) Display the template that maximizes system resources for IPv4 static routing on SVIs.
qos	(Optional) Display the template that maximizes system resources for quality of service (QoS) access control entries (ACEs).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)FX	This command was introduced.
12.2(40)SE	The **dual-ipv4-and-ipv6 default** keywords were added.
12.2(53)SE1	The **default** template for the Catalyst 2960-S switch was added.
12.2(55)SE	The **lanbase-routing** template was added for static routing on SVIs.
12.2(55)EX	The Catalyst 2960-C templates were added.

Usage Guidelines

When you change the SDM template on a switch by using the **sdm prefer** global configuration command, you must reload the switch for the configuration to take effect. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

A Catalyst 2960-S switch running the LAN base image uses a default template that includes maximum resources for all supported features or the lanbase-routing template to enable static routing.

Catalyst 2960-C Gigabit Ethernet switches use only a default template for maximum resource support.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured.

All Catalyst 2960-C switches support 0 routed interfaces and 255 VLANs.

Examples

This is an example of output from the **show sdm prefer default** command on a Catalyst 2960 switch:

```
Switch# show sdm prefer default
 "default" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                 8K
  number of IPv4 IGMP groups:                      256
  number of IPv4/MAC qos aces:                     128
  number of IPv4/MAC security aces:                384
```

This is an example of output from the **show sdm prefer** command on a Catalyst 2960 switch showing the existing template:

```
Switch# show sdm prefer
The current template is "lanbase-routing" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                  4K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    4.25K
    number of directly-connected IPv4 hosts:        4K
    number of indirect IPv4 routes:                 0.25K
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.125k
  number of IPv4/MAC security aces:                 0.375k
```

This is an example of output from the **show sdm prefer default** command on a Catalyst 2960-S switch:

```
Switch# show sdm prefer default
 "default" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups:                       0.25K
  number of IPv6 multicast groups:                  0.25K
  number of IPv4/MAC qos aces:                      0.375k
  number of IPv4/MAC security aces:                 0.375k
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          0
  number of IPv6 security aces:                     0.125k
```

This is an example of output from the **show sdm prefer qos** command on a Catalyst 2960 switch:

```
Switch# show sdm prefer qos
 "qos" template:
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                8K
  number of IPv4 IGMP groups:                     256
  number of IPv4/MAC qos aces:                    384
  number of IPv4/MAC security aces:               128
```

This is an example of output from the **show sdm prefer** command on a Catalyst 2960-C Gigabit Ethernet switch:

```
Switch# show sdm prefer qos
The current template is "default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 255 VLANs.

  number of unicast mac addresses:                 8K
  number of IPv4 IGMP groups:                      0.25K
  number of IPv6 multicast groups:                 0.25K
  number of IPv4/MAC qos aces:                     0.125k
  number of IPv4/MAC security aces:                0.375k
  number of IPv6 policy based routing aces:        0
  number of IPv6 qos aces:                         60
  number of IPv6 security aces:                    0.125k
```

Updates to the Catalyst 2960 System Message Guide

These system messages are new for the Catalyst 2960-C switch:

Error Message `CDP_PD-2-POWER_LOW: 15.4 W power - NEGOTIATED [char] on port [char]`

Explanation Power is being received on the uplink ports, and the power source has negotiated a power level that is 15.4 W The first [char] is the device providing power, and the second [char] is the uplink port or ports.

Recommended Action No action is required.

Error Message `CDP_PD-4-POWER_OK: 30 W power - NEGOTIATED [char] on port [char]`

Explanation Power is being received on the uplink ports, and the power source has negotiated a power level that is the maximum of 30 W. The first [char] is the device providing power, and the second [char] is the uplink port or ports.

Recommended Action No action is required.

Error Message `PDPSE-5-PWR_SRC_DISC: Power source change from [chars] to [chars]. Current power source is [chars]`

Explanation A new power source, either auxiliary power or through the uplink ports, was discovered, causing a power source change. The first [chars] is the previous power source (port number of the uplink port or auxiliary power), the second [chars] is the discovered power source (uplink port number or auxiliary power). The third [chars] is the power source that is being used.

Recommended Action No action is required.

Related Documentation

These documents with information about the Catalyst 2960-C switches are available on Cisco.com:

http://www.cisco.com/en/US/products/ps11290/tsd_products_support_series_home.html

- *Catalyst 2960-C and 3560-C Switch Hardware Installation Guide*
- *Catalyst 2960-C and 3560-C Switch Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 2960-C and 3560-C Switch*

These documents with information about the Catalyst 2960-S and 2960 switches are available at Cisco.com:
http://www.cisco.com/en/US/products/ps6406/tsd_products_support_series_home.html

- *Catalyst 2960 and 2960-S Switch Software Configuration Guide*
- *Catalyst 2960 and 2960-S Switch Command Reference*
- *Catalyst 3750, 3560, 3550, 2975, 2970, 2960, and 2960-S Switch System Message Guide*

For other information about related products, see these documents:

- *Smart Install Configuration Guide*
- *Auto Smartports Configuration Guide*
- *Cisco EnergyWise Configuration Guide*
- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- For more information about the Network Admission Control (NAC) features, see the *Network Admission Control Software Configuration Guide*
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site: http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  SFP compatibility matrix documents are available from this Cisco.com site: http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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