Release Notes for the Cisco EtherSwitch Service Modules, Cisco IOS Release 12.2(25)EZ and Later

Revised August 1, 2005

The Cisco IOS Release 12.2(25)EZ and later runs on all Cisco EtherSwitch Service Modules.

The Cisco EtherSwitch service modules and Catalyst 3750 switches support stacking through Cisco StackWise technology.

These release notes include important information about Cisco IOS Release 12.2(25)EZ and Cisco IOS Release 12.2(25)EZ1, and any limitations, restrictions, and caveats that apply to them. 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.

For the complete list of Cisco EtherSwitch service module or Catalyst 3750 switch documentation, see the "Related Documentation" section on page 41.

You can download the switch software from this site (registered Cisco.com users with a login password):

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

Note For IPv6 capability on the Cisco EtherSwitch service modules and Catalyst 3750 switches, you must order the advanced IP services image upgrade from Cisco.

This software release is part of a special release of Cisco IOS software. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Cisco IOS Release 12.2(25)EZ and later is based on Cisco IOS Release 12.2(25)SEB. Open caveats in Cisco IOS Release 12.2(25)SEB also affect Cisco IOS Release 12.2(25)EZ and later.

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

Contents

This information is in the release notes:

System Requirements

The system requirements are described in these sections:

- "Hardware Supported" section on page 3
- "Device Manager System Requirements" section on page 3
- "Cluster Compatibility" section on page 4

Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2(25)EZ.

Table 1 Cisco EtherSwitch Service Modules Supported Hardware

Cisco EtherSwitch Service Module	Description	Supported by Minimum Cisco IOS Release
NME-16ES-1G-P	16 10/100 PoE[1] ports, 1 10/100/1000 Ethernet port, no StackWise connector ports, single-wide	Cisco IOS Release 12.2(25)EZ
NME-X-23ES-1G-P	23 10/100 PoE ports, 1 10/100/1000 PoE port, no StackWise connector ports, extended single-wide	Cisco IOS Release 12.2(25)EZ
NME-XD-24ES-1S-P	24 10/100 PoE ports, 1 SFP[2] port, 2 StackWise connector ports, extended double-wide	Cisco IOS Release 12.2(25)EZ
NME-XD-48ES-2S-P	48 10/100 PoE ports, 2 SFP ports, no StackWise connector ports, extended double-wide	Cisco IOS Release 12.2(25)EZ
SFP modules	1000BASE-T, 1000BASE-SX 1000BASE-LX, 1000BASE-ZX, CWDM[3], and 100BASE-FX MMF[4]	Cisco IOS Release 12.2(25)EZ

[1] PoE = Power over Ethernet

[2] SFP = small form-factor pluggable

[3] CWDM = coarse wavelength-division multiplexer

[4] MMF = multimode fiber

Device Manager System Requirements

These sections describes the hardware and software requirements for using the device manager:

- "Hardware Requirements" section on page 3
- "Software Requirements" section on page 4

Hardware Requirements

Table 2 lists the minimum hardware requirements for running the device manager.

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II[1]	64 MB[2]	256	1024 x 768	Small

[1] We recommend Intel Pentium 4.

[2] We recommend 256-MB DRAM.

Software Requirements

Table 3 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.

Note The device manager does not require a plug-in.

Table 3 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer[1]	Netscape Navigator
Windows 98	None	5.5 or 6.0	7.1
Windows NT 4.0	Service Pack 6 or later	5.5 or 6.0	7.1
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

[1] Service Pack 1 or higher is required for Internet Explorer 5.5.

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Cisco EtherSwitch StackWise Service Module or Catalyst 3750 switch, all standby command switches must be Cisco EtherSwitch StackWise Service Modules or Catalyst 3750 switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the Cisco EtherSwitch service module feature guide, and the Catalyst 3750 software configuration guide and command reference.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- "Finding the Software Version and Feature Set" section on page 5
- "Deciding Which Files to Use" section on page 5
- "Upgrading a Switch by Using the Device Manager or Network Assistant" section on page 6
- "Upgrading a Switch by Using the CLI" section on page 7
- "Recovering from a Software Failure" section on page 8

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.

Note For Cisco EtherSwitch service modules, although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base image [formerly known as the SMI] or IP services image [formerly known as the EMI]) and does not change if you upgrade the software image.

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

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 command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Cisco IOS Release 12.2(25)EZ refers to the SMI as the *IP base* image and the EMI as the *IP services* image.

Table 4 lists the different file-naming conventions for the Cisco IOS Release 12.2(25)EZ and later.

Table 4 Cisco IOS Image File Naming Convention

Cisco IOS 12.2(25)EZ and later
c3750-ipbase-mz
c3750-ipbasek9-mz
c3750-ipservices-mz
c3750-ipservicesk9-mz
c3750-advipservicesk9-mz

Table 5 lists the filenames for this software release.

Note For IPv6 capability on the Cisco EtherSwitch service module and Catalyst 3750 switches, you must order the advanced IP services image upgrade from Cisco.

Table 5 Cisco IOS Software Image Files

Filename	Description
c3750-ipbase-tar.122-25.EZ.tar	Catalyst 3750 IP base image and device manager files. This image has Layer 2+ and basic Layer 3 routing features.
c3750-ipservices-tar.122-25.EZ.tar	Catalyst 3750 IP services image and device manager files. This image has both Layer 2+ and full Layer 3 routing features.
c3750-ipbasek9-tar.122-25.EZ.tar	Catalyst 3750 IP base cryptographic image and device manager files. This image has the Kerberos, SSH[1], Layer 2+, and basic Layer 3 routing features.
c3750-ipservicesk9-tar.122-25.EZ.tar	Catalyst 3750 IP services cryptographic image and device manager files. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 features.
c3750-advipservicesk9-tar.122-25.EZ1.tar	Catalyst 3750 advanced IP services image, cryptographic file, and device manager files. This image has all the IP services image (formerly known as the EMI) features and the capability for unicast routing of IPv6 packets.

[1] SSH = Secure Shell

Upgrading a Switch by Using the Device Manager or Network Assistant

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 5 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

To download the image for a Catalyst 2970 switch, click **Catalyst 2970 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 2970 3DES Cryptographic Software**.

To download the IP services image (formerly known as the EMI) or IP base image (formerly known as the SMI) files for a Catalyst 3560 switch, click **Catalyst 3560 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560 3DES Cryptographic Software**.

To download the IP services image (formerly known as the EMI) or IP base image (formerly known as the SMI) files for a Catalyst 3750 switch, click **Catalyst 3750 software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3750 3DES Cryptographic Software**.

Caution If you are upgrading a Catalyst 3750 or a Catalyst 2970 switch that is running a release earlier than Cisco IOS Release 12.1(19)EA1c, this release includes a bootloader upgrade. The bootloader can take up to 1 minute to upgrade the first time that the new software is loaded. Do not power cycle the switch during the bootloader upgrade.

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 (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, 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 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/c3750-ipservices-tar.122-25.SEB.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 recovery procedures, see 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, 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.

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 Hardware Features

For a list of all supported hardware, see the “Hardware Supported” section on page 3.

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.

This section contains these limitations:

- "Cisco IOS Limitations" section on page 9
- "Device Manager Limitations" section on page 19

Cisco IOS Limitations

These limitations apply to the Cisco EtherSwitch service modules or Catalyst 3750 switches:

- "Configuration" section on page 9
- "Ethernet" section on page 11
- "Fallback Bridging" section on page 12
- "HSRP" section on page 12
- "IP" section on page 12
- "IP Telephony" section on page 12
- "MAC Addressing" section on page 13
- "Multicasting" section on page 13
- "QoS" section on page 15
- "Routing" section on page 15
- "SPAN and RSPAN" section on page 16
- "Stacking (Cisco EtherSwitch service module switch stack and Catalyst 3750 switch stack)" section on page 17
- "Trunking" section on page 18
- "VLAN" section on page 18

Configuration

These are the configuration limitations:

- 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. (CSCea71176 and CSCdz11708)

- When you change a port from a nonrouted port to a routed port or the reverse, the applied auto-QoS setting is not changed or updated when you verify it by using the **show running interface** or **show mls qos interface** user EXEC commands. These are the workarounds:

  1. Disable auto-QoS on the interface.
  2. Change the routed port to a nonrouted port or the reverse.
  3. Re-enable auto-QoS on the interface. (CSCec44169)

- The DHCP snooping binding database is not written to flash memory or a remote file in any of these situations:

  - When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and the peer work correctly.
  - The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is manually removed from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - The URL for the configured DHCP snooping database was replaced because the original URL was not accessible. The new URL might not take effect after the timeout of the old URL.

  No workaround is necessary; these are the designed behaviors. (CSCed50819)

- When dynamic ARP inspection is enabled on a switch or switch stack, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

  However, when dynamic ARP inspection is not enabled and a jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mbps full duplex or 100 Mbps 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 Mbps and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails are lost.

  When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which you entered the command.

  There is no workaround. (CSCed95822)

- 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)

- (Cisco EtherSwitch service modules) Console baud rate changes in switch IOS are not allowed. The console on the Cisco Etherswitch Service module only supports three baud rates (9600 bps, 19200 bps and 38400 bps) and must be set at the bootloader prompt. Changing baud rates in the switch IOS is not allowed and the command will be rejected.

To change the baud rate, reload the Cisco Etherswitch Service module to the bootloader prompt. Then, change the baud rate and change the speed on the TTY line of the router connecting to the Cisco Etherswitch Service module console.

There is no workaround. (CSCeh50152)

- (Cisco EtherSwitch service modules) The bootloader defaults to read-only mode after the password recovery is performed. When password recovery procedure is completed, the bootloader changes into read only mode. After this, anything configured at the bootloader prompt will be lost when the switch is reset.

  The workaround is after password recovery is completed, at the Cisco Etherswitch Service module, prompt, configure it to read-write mode with **set_bs bs: rw** before setting any variable and then enter **set_param** to write the changes before resetting the Cisco Etherswitch Service module. (CSCeh45594)

Ethernet

These are the Ethernet limitations:

- Subnetwork Access Protocol (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)
- Link connectivity might be lost between some older models of the Intel Pro1000 NIC and the 10/100/1000 switch port interfaces. The loss of connectivity occurs between the NIC and Cisco EtherSwitch service module Gigabit Ethernet ports.

  These are the workarounds:

  - Contact the NIC vendor, and obtain the latest driver for the card.
  - Configure the interface for 1000 Mbps instead of for 10/100 Mbps.
  - Connect the NIC to an interface that is not listed here. (CSCea77032)

  For more information, enter *CSCea77032* in the Bug Toolkit at this URL:

  http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl
- (Cisco EtherSwitch service modules) When the Cisco EtherSwitch service module is reloaded or the internal link is reset, depending on the configuration, there can be up to a 45-second delay in providing power to PoE devices. If the internal Gigabit Ethernet interface on the Cisco EtherSwitch service module connected to the router is configured as a switchport (access or trunk mode), the internal link will not be operational until it reaches the STP forwarding state. Therefore, the PoE that has to come from the host router will also not be available until the internal Gigabit Ethernet link reaches the STP forwarding state. This is due to due to STP convergence time. This problem does not occur on routed ports.

  The workaround is when the Cisco EtherSwitch service module is in access mode, configure **spanning-tree portfast** on the internal Gigabit Ethernet interface. If it is in trunk mode, there is no workaround.

Fallback Bridging

These are the fallback bridging limitations:

- If a bridge group contains a VLAN to which a static MAC address is configured, all non-IP traffic in the bridge group with this MAC address destination is sent to all ports in the bridge group. The workaround is to remove the VLAN from the bridge group or to remove the static MAC address from the VLAN. (CSCdw81955)
- Known unicast (secured) addresses are flooded within a bridge group if secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group. Non-IP traffic destined to the secure addresses is flooded within the bridge group. The workaround is to disable fallback bridging or to disable port security on all ports in all VLANs participating in fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group** *bridge-group* interface configuration command. To disable port security on all ports in all VLANs participating in fallback bridging, use the **no switchport port-security** interface configuration command. (CSCdz80499)

HSRP

This is the Hot Standby Routing Protocol (HSRP) limitation:

When the active switch fails in a switch cluster that uses HSRP redundancy, the new active switch might not contain a full cluster member list. The workaround is to ensure that the ports on the standby cluster members are not in the spanning-tree blocking state. To verify that these ports are not in the blocking state, see the "Configuring STP" chapter in the software configuration guide. (CSCec76893)

IP

These are the IP limitations:

- The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out. The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)
- 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)

IP Telephony

These are the IP telephony limitations:

- Some access point (AP)-350 devices are incorrectly discovered as IEEE 802.3af Class 1 devices. These APs should be discovered as Cisco pre-standard devices. The **show power inline** user EXEC command shows the AP-350 as an IEEE Class 1 device. The workaround is to power the AP by using an AC wall adaptor. (CSCin69533)
- When a Cisco IP Phone is connected to the switch, the port VLAN ID (PVID) and the voice VLAN ID (VVID) both learn its MAC address. However, after dynamic MAC addresses are deleted, only the VVID relearns the phone MAC address. MAC addresses are manually or automatically deleted when a topology change occurs or when port security or an IEEE 802.1x feature is enabled or disabled. There is no workaround. (CSCea80105)

- 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)
- The switch uses the IEEE classification to learn the maximum power consumption of a powered device before powering it. The switch grants power only when the maximum wattage configured on the port is less than or equal to the IEEE class maximum. This ensures that the switch power budget is not oversubscribed. There is no such mechanism in Cisco prestandard powered devices.

  The workaround for networks with pre-standard powered devices is to leave the maximum wattage set at the default value (15.4 W). You can also configure the maximum wattage for the port for no less than the value the powered device reports as the power consumption through CDP messages. For networks with IEEE Class 0, 3, or 4 devices, do not configure the maximum wattage for the port at less than the default 15.4 W (15,400 milliwatts). (CSCee80668)

MAC Addressing

This is the MAC addressing limitation:

When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

Multicasting

These are the multicasting limitations:

- The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)
- 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)
- When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)

- If the stack master is power cycled immediately after you enter the **ip mroute** global configuration command, there is a slight chance that this configuration change might be lost after the stack master changes. This occurs because the stack master did not have time to propagate the running configuration to all the stack members before it was powered down. This problem might also affect other configuration commands. There is no workaround. (CSCea71255)
- When you enable IP Protocol-Independent Multicast (PIM) on a tunnel interface, the switch incorrectly displays the `Multicast is not supported on tunnel interfaces` error message. IP PIM is not supported on tunnel interfaces. There is no workaround. (CSCeb75366)
- 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)

Power

- When used power is displayed on the Cisco EtherSwitch service module by issuing the **show power inline** command, total used power is displayed by all Cisco EtherSwitch service modules in the router. Any remaining power shown is the remaining power available for allocation to switching ports on all Cisco EtherSwitch service modules in the router. When the total power just used, by particular EtherSwitch service module, is displayed on an EtherSwitch Service module interface by entering the **show power inline** command on the router, the following is displayed:

```
Router#sh power inline
PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
INT-PS           0       360.000   121.000         PS1 GOOD   PS2 ABSENT
Interface   Config   Device    Powered    PowerAllocated
---------   ------   ------    -------    --------------
Gi4/0       auto     Unknown  On        121.000 Watts
```

  This is not a problem. It is the correct method used to show the total used power and the remaining power available on the system. (CSCeg74337)

QoS

These are the quality of service (QoS) limitations:

- 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)

Routing

These are the routing limitations:

- The switch does not support tunnel interfaces for unicast routed traffic. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnel interfaces are supported for multicast routing.
- A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported. There is no workaround. (CSCea52915)
- On a Cisco EtherSwitch service module switch stack or Catalyst 3750 switch stack with a large number of switched virtual interfaces (SVIs), routes, or both on a fully populated nine-member switch stack, this message might appear when you reload the switch stack or add a switch to the stack:

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

  This error message means there is a temporary memory shortage that normally recovers by itself. You can verify that the switch stack has recovered by entering the **show cef line** user EXEC command and verifying that the line card states are `up` and `sync`. No workaround is required because the problem is self-correcting. (CSCea71611)
- A spanning-tree loop might occur if all of these conditions are true:
  - Port security is enabled with the violation mode set to protected.
  - The maximum number of secure addresses is less than the number of switches connected to the port.
  - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

  The workaround is to change any one of the listed conditions. (CSCed53633)

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the **replicate** option. For a remote SPAN session, there is no workaround (CSCdy72835).
- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the RSPAN VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the **encapsulation replicate** option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround (CSCdy81521).
- 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).
- (Cisco EtherSwitch service modules or Catalyst 3750 switches) The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)
- On Cisco EtherSwitch service modules or Catalyst 3750 switches, some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)
- 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)

Stacking (Cisco EtherSwitch service module switch stack and Catalyst 3750 switch stack)

These are the Cisco EtherSwitch service module switch stack or Catalyst 3750 switch stack limitations:

- If the stack master is immediately reloaded after adding multiple VLANs, the new stack master might fail. The workaround is to wait a few minutes after adding VLANs before reloading the stack master. (CSCea26207)
- If the console speed is changed on a stack, the configuration file is updated, but the baud rate is not. When the switch is reloaded, meaningless characters might appear on the console during bootup before the configuration file is parsed and the console speed is set to the correct value. If manual boot is enabled or the startup configuration is deleted after you change the console speed, you cannot access the console after the switch reboots. There is no workaround. (CSCec36644)
- If a switch is forwarding traffic from a Gigabit ingress interface to a 100 Mbps egress interface, the ingress interface might drop more packets due to oversubscription if the egress interface is on a Fast Ethernet switch. There is no workaround. (CSCed00328)
- If a stack member is removed from a stack and either the configuration is not saved or another switch is added to the stack at the same time, the configuration of the first member switch might be lost. The workaround is to save the stack configuration before removing or replacing any switch in the stack. (CSCed15939)
- When the **switchport** and **no switchport** interface configuration commands are entered more than 20,000 times on a port of a Cisco EtherSwitch service module or Catalyst 3750 switch, all available memory is used, and the switch halts.

  There is no workaround. (CSCed54150)
- In a private-VLAN domain, only the default private-VLAN IP gateways have sticky ARP enabled. The intermediate Layer 2 switches that have private VLAN enabled disable sticky ARP. When a stack master switch-over occurs on one of the Cisco EtherSwitch service modules or Catalyst 3750 default IP gateways, the message `IP-3-STCKYARPOVR` appears on the consoles of other default IP gateways. Because sticky ARP is not disabled, the MAC address update caused by the stack master switch-over cannot complete.

  The workaround is to complete the MAC address update by entering the **clear arp** privileged EXEC command. (CSCed62409)
- When a Cisco EtherSwitch service module or Catalyst 3750 switch is being reloaded in a switch stack, packet loss might occur for up to 1 minute while the Cisco Express Forwarding (CEF) table is downloaded to the switch. This only impacts traffic that will be routed through the switch that is being reloaded. There is no workaround. (CSCed70894)
- Inconsistent private-VLAN configuration can occur on a switch stack if a new stack master is running the IP base image and the old stack master was running the IP services image.

  Private VLAN is enabled or disabled on a switch stack, depending on whether or not the stack master is running the IP services image or the IP base image:

  - If the stack master is running the IP services image, all stack members have private VLAN enabled.
  - If the stack master is running the IP base image, all stack members have private VLAN disabled.

  This occurs after a stack master re-election when the previous stack master was running the IP services image and the new stack master is running the IP base image. The stack members are configured with private VLAN, but any new switch that joins the stack will have private VLAN disabled.

  These are the workarounds. Only one of these is necessary:

  - Reload the stack after an IP services image to IP base image master switch change (or the reverse).
  - Before an IP services image-to-IP base image master switch change, delete the private-VLAN configuration from the existing stack master. (CSCee06802)
- Port configuration information is lost when changing from **switchport** to **no switchport** modes on Catalyst 3750 switches.

  This is the expected behavior of the offline configuration (provisioning) feature. There is no workaround. (CSCee12431)

Trunking

These are the trunking limitations:

- 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).
- If a Catalyst 3750 switch stack is connected to a designated bridge and the root port of the switch stack is on a different switch than the alternate root port, changing the port priority of the designated ports on the designated bridge has no effect on the root port selection for the Catalyst 3750 switch stack. There is no workaround. (CSCea40988)
- 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

These are the VLAN limitations:

- 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)
- A CPUHOG message sometimes appears when you configure a private VLAN. Enable port security on one or more of the ports affected by the private VLAN configuration.

  There is no workaround. (CSCed71422)
- When you apply a per-VLAN quality of service (QoS), per-port policer policy-map to a VLAN Switched Virtual Interface (SVI), the second-level (child) policy-map in use cannot be re-used by another policy-map.

  The workaround is to define another policy-map name for the second-level policy-map with the same configuration to be used for another policy-map. (CSCef47377)

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

These sections describe the important notes related to this software release for the Cisco EtherSwitch service modules or Catalyst 3750 switches:

- "Switch Stack Notes" section on page 19
- "Device Manager Notes" section on page 19

Switch Stack Notes

These notes apply to switch stacks:

- Always power off a switch before adding or removing it from a switch stack.
- Catalyst 3750 switches running Cisco IOS Release 12.2(25)SEB are compatible with Cisco EtherSwitch service modules running Cisco IOS Release 12.2(25)EZ. Catalyst 3750 switches and Cisco EtherSwitch service modules can be in the same switch stack. In this switch stack, the Catalyst 3750 switch or the Cisco EtherSwitch service module can be the stack master.

Device Manager Notes

These notes apply to the device manager:

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- The Legend on the device manager incorrectly includes the 1000BASE-BX SFP module.
- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

  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** {**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.

- 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:

	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.

- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.cisco.com:84*), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.

Open Caveats

This section describes the open caveats with possible unexpected activity in this software release. Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Cisco EtherSwitch service modules or Catalyst 3750 switches:

- CSCee71979 (Cisco EtherSwitch service modules)

  Non-PoE devices attached to a network are erroneously detected as IEEE PD occasionally and powered by the Cisco Etherswitch service module.

  There is no workaround, It is recommended to configure **power inline never** on the Cisco Etherswitch service module ports that do not have PoE device connected.

- CSCee96492 (Cisco EtherSwitch service modules)

  When booting up, some non-harmful messages related to stacking may display although the Cisco Etherswitch service module is not capable of stacking.

  There is no workaround.

- CSCef37624

  You cannot ping a Layer 3 interface that has a Network Address Translation (NAT) configuration.

  There is no workaround.

  Problem:

- CSCef84975 (Cisco EtherSwitch service modules)

  Phone detect events, generated by many IEEE phones connected to switch ports, can consume a significant amount of CPU time. However, the switch ports cannot power the phones because the internal link is down.

  The workaround is, if the problem persists, to enter the **power inline never** command on all the FE ports that are not powered but connected to IP phones,

- CSCef94884

  Disabling OSPFv3 causes a memory leak.

  There is no workaround.

- CSCeg27382

  If the per-VLAN QoS per-port policer policy-map is already attached to a VLAN switched virtual interface (SVI), do not modify the second level (port-level) policy-map. If you modify the policy-map by removing the policer while it is still attached, an error message appears, and the policy-map is detached by the switch. The policer cannot be re-applied back to that policy-map.

  The workaround is to redefine the second-level (port level) policy map if the policy map has already been detached by the system.

- CSCeg53353 (Cisco EtherSwitch service modules)

  Static power allocation on an Etherswitch Service module port is not supported in this release.

  There is no workaround.

- CSCeg56931 (Cisco EtherSwitch service modules)

  The Etherswitch service module randomly does not power some ports during a power cycle. This issue will be resolved in IOS software release 12.3(14)T1 and later versions.

- CSCeh01250 (Cisco EtherSwitch service modules)

When connected to the router through an auxiliary port in a session to the Cisco EtherSwitch service module, by entering the **shut/no shut** command on the service module router interface, the service module session will fail.

The workaround is to reload the router or connect to router through the console and open a session to the service module.

- CSCeh15112

  When IEEE 802.1x is enabled on one or more ports of a member switch and you enter the **show dot1x all** privileged EXEC command, the command output does not have IEEE 802.1x information about ports on the member switches.

  The workaround is to use the **show dot1x interface** privileged EXEC command to display the information for a specific interface.

- CSCeh16869

  In an multiple spanning-tree (MST) region in which Switch 1 is connected to Switch 2 and Switch 2 is connected to Switch 3, if Switch 2 has a root port and a designated port in MST instance 2, the root port flaps. The designated port is not synchronized with the other switches in the MST region, and the convergence of the port from the blocking state to the learning state is slow.

  The workaround is to modify the switch priority to a lower value so that the Switch 2 becomes the root switch for the MST instances 0 and 2.

- CSCeh19672

  If an IEEE 802.1x client configured for both machine and user authentication is connected to a Cisco EtherSwitch service module or Catalyst 3750 switch running Cisco IOS Release 12.2(25)SE and RADIUS VLAN assignment is used only for the machine authentication, the user might take 2 to 5 minutes to authenticate.

  Use one of these workarounds:

  - Use the same VLAN for machine and user authentication.
  - If the same VLAN cannot be used, reduce the quiet period by using the **dot1x timeout quiet-period** *seconds* interface configuration command.

- CSCeh35595 (Cisco EtherSwitch service module)

  A duplex mismatch occurs when two FE interfaces, connected back to back on two EtherSwitch service modules, are configured as 100/full and auto/auto. This is expected behavior for the PHY on the Cisco Etherswitch service module.

  There is no workaround.

- CSCeh35693 (Cisco EtherSwitch service modules)

  If two Cisco EtherSwitch service modules are connected back to back via FE interfaces configured as 100/full and auto/auto, one FE may detect the FE other as Cisco PD.

  There is no workaround.

- CSCeh45465 (Cisco EtherSwitch service modules)

  Entering the **shut/no shut** command 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 will not get inline power if the internal link is brought up within 5 minutes.

  The workaround is to issue the **shut/no shut** command on the FE interface of a new IP phone is attached to after the internal link is brought up once again.

- CSCeh46718 (Cisco EtherSwitch service modules)

SFP-100FX modules do not work on a 48-port Cisco EtherSwitch service module.

There is no workaround.

- CSCeh52964 (Cisco EtherSwitch service modules)

  Sometimes when the router is rebooted after power on (approximately once in 10 to 15 reboots), the Router Blade Communication Protocol (RBCP) between the router and the EtherSwitch service module may not be reestablished. In this situation, the following error message is displayed:

  ```
  [date]: %Y88E8K-3-ILP_MSG_TIMEOUT_ERROR: GigabitEthernet1/0: EtherSwitch Service
        Module RBCP ILP messages timeout
  ```

  The workaround is to reload the EtherSwitch service module software without rebooting the router. The switching software may be reloaded by using the **reload** command at the EtherSwitch service module prompt or running the **service-module g** <*slot#*>*/0* **reset** command at the router prompt.

Resolved Caveats

This section describes the caveats that have been resolved in release 12.2(25)EZ1. Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the Cisco EtherSwitch service modules or Catalyst 3750 switches:

- CSCef68324

  Cisco Internetwork Operating System (IOS) software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

  Cisco has made free software available to address this vulnerability for all affected customers.

  More details can be found in the security advisory that is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050729-ipv6.shtml.

Documentation Updates in Cisco IOS Release 12.2(25)EZ

These are the updates to the product documentation that occurred in Cisco IOS Release 12.2(25)EZ.

Updates to the Software Configuration Guides

This section contains these updates to the switch software configuration guides:

- "Supported MIBs" section on page 24
- "Port Security Updates" section on page 24
- "IGMP Updates" section on page 28
- "QoS Updates" section on page 30

Supported MIBs

In Appendix A, "Supported MIBs," the "Using FTP to Access the MIB Files" section was revised. This is the correct procedure.

You can obtain each MIB file by using this procedure:

Step 1 Make sure that your FTP client is in passive mode.

Note Some FTP clients do not support passive mode.

Step 2 Use FTP to access the server ftp.cisco.com.

Step 3 Log in with the username **anonymous**.

Step 4 Enter your e-mail username when prompted for the password.

Step 5 At the `ftp>` prompt, change directories to /pub/mibs/v1 and /pub/mibs/v2.

Step 6 Use the get MIB_filename command to get a copy of the MIB file.

Port Security Updates

The port security section was changed in the "Configuring Port-Based Traffic Control" chapter to include port security on voice VLANs. These sections are revised:

- "Port Security Configuration Guidelines" section on page 24
- "Enabling and Configuring Port Security" section on page 25

Port Security Configuration Guidelines

Follow these guidelines when configuring port security:

- Port security can only be configured on static access ports or trunk ports. A secure port cannot be a dynamic access port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or a Gigabit EtherChannel port group.

Note Voice VLAN is only supported on access ports and not on trunk ports, even though the configuration is allowed.

- A secure port cannot be a private-VLAN port. (Catalyst 3750 and 3560 only)
- When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP Phone, the IP phone requires up to two MAC addresses. The IP phone address is learned on the voice VLAN and might also be learned on the access VLAN. Connecting a PC to the IP phone requires additional MAC addresses.

- When you enter a maximum secure address value for an interface, and the new value is greater than the previous value, the new value overwrites the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

Table 6 summarizes port security compatibility with other port-based features.

Table 6 Port Security Compatibility with Other Switch Features

Type of Port or Feature on Port	Compatible with Port Security
DTP[1] port[2]	No
Trunk port	Yes
Dynamic-access port[3]	No
Routed port (Catalyst 3750 and 3560 only)	No
SPAN source port	Yes
SPAN destination port	No
EtherChannel	No
Tunneling port (Catalyst 3750 and 3560 only)	Yes
Protected port	Yes
IEEE 802.1x port	Yes
Voice VLAN port[4]	Yes
Private VLAN port (Catalyst 3750 and 3560 only) **Note** The switch must be running the IP services image (formerly known as the EMI).	No
IP source guard (Catalyst 3750 and 3560 only)	Yes
Dynamic ARP[5] inspection (Catalyst 3750 and 3560 only)	Yes
Flex Links	Yes

[1] DTP = Dynamic Trunking Protocol

[2] A port configured with the **switchport mode dynamic** interface configuration command.

[3] A VLAN Query Protocol (VQP) port configured with the **switchport access vlan dynamic** interface configuration command.

[4] You must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN.

[5] ARP = Address Resolution Protocol

Enabling and Configuring Port Security

Beginning in privileged EXEC mode, follow these steps to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface to be configured, and enter interface configuration mode.

	Command	Purpose
Step 3	**switchport mode** {**access** | **trunk**}	Set the interface switchport mode as access or trunk. An interface in the default mode (dynamic auto) cannot be configured as a secure port.
Step 4	**switchport voice vlan** *vlan-id*	Enable voice VLAN on a port. *vlan-id*—Specify the VLAN to be used for voice traffic.
Step 5	**switchport port-security**	Enable port security on the interface.
Step 6	**switchport port-security** [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]	(Optional) Set the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. On the Catalyst 3750 and 3560, the number is set by the active Switch Database Management (SDM) template. See Chapter 8, "Configuring SDM Templates." This number is the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces. (Optional) **vlan**—set a per-VLAN maximum value Enter one of these options after you enter the **vlan** keyword: • *vlan-list*—On a trunk port, you can set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used. • **access**—On an access port, specify the VLAN as an access VLAN. • **voice**—On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

	Command	Purpose
Step 7	**switchport port-security violation** {**protect** | **restrict** | **shutdown**}	(Optional) Set the violation mode, the action to be taken when a security violation is detected, as one of these: • **protect**—When the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. **Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit. • **restrict**—When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. • **shutdown**—The interface is error-disabled when a violation occurs, and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. **Note** When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands.
Step 8	**switchport port-security** [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}]	(Optional) Enter a secure MAC address for the interface. You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned. **Note** If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration. (Optional) **vlan**—set a per-VLAN maximum value. Enter one of these options after you enter the **vlan** keyword: • *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • **access**—On an access port, specify the VLAN as an access VLAN. • **voice**—On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.
Step 9	**switchport port-security mac-address sticky**	(Optional) Enable sticky learning on the interface.

	Command	Purpose
Step 10	**switchport port-security mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]	(Optional) Enter a sticky secure MAC address, repeating the command as many times as necessary. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned, are converted to sticky secure MAC addresses, and are added to the running configuration. **Note** If you do not enable sticky learning before this command is entered, an error message appears, and you cannot enter a sticky secure MAC address. (Optional) **vlan**—set a per-VLAN maximum value. Enter one of these options after you enter the **vlan** keyword: • *vlan-id*—On a trunk port, you can specify the VLAN ID and the MAC address. If you do not specify a VLAN ID, the native VLAN is used. • **access**—On an access port, specify the VLAN as an access VLAN. • **voice**—On an access port, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**show port-security**	Verify your entries.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to enable sticky port security on a port, to manually configure MAC addresses for data VLAN and voice VLAN, and to set the total maximum number of secure addresses to 20 (10 for data VLAN and 10 for voice VLAN).

```
Switch(config)# interface FastEthernet1/0/1
Switch(config-if)# switchport access vlan 21
Switch(config-if)# switchport mode access
Switch(config-if)# switchport voice vlan 22
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 20
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0002
Switch(config-if)# switchport port-security mac-address 0000.0000.0003
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice
Switch(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
Switch(config-if)# switchport port-security maximum 10 vlan access
Switch(config-if)# switchport port-security maximum 10 vlan voice
```

IGMP Updates

The configurable IGMP leave timer was added to the “Configuring IGMP Snooping” chapter in this release. These sections describe the timer:

- “Understanding the IGMP Configurable-Leave Timer” section on page 29
- “IGMP Leave Timer Guidelines” section on page 29
- “Configuring the IGMP Leave Timer” section on page 29

Understanding the IGMP Configurable-Leave Timer

In Cisco IOS Release 12.2(25)SEA and earlier, the IGMP snooping leave time was fixed at 5 seconds. If membership reports were not received by the switch before the query response time expired, a port was removed from the multicast group membership. However, some applications require a leave latency of less than 5 seconds.

In Cisco IOS Release 12.2(25)SEB and later, you can configure the time that the switch waits after sending a group-specific query to determine if hosts are still interested in a specific multicast group. The IGMP leave response time can be configured from 100 to 5000 milliseconds. The timer can be set either globally or on a per-VLAN basis. The VLAN configuration of the leave time overrides the global configuration.

IGMP Leave Timer Guidelines

Follows these guidelines when configuring the IGMP leave timer:

- You can configure the leave time globally or on a per-VLAN basis.
- Configuring the leave time on a VLAN overrides the global setting.
- The default leave time is 1000 milliseconds.
- The IGMP configurable leave time is only supported on hosts running IGMP Version 2.
- The actual leave latency in the network is usually the configured leave time. However, the leave time *might* vary around the configured time, depending on real-time CPU load conditions, network delays and the amount of traffic sent through the interface.

Configuring the IGMP Leave Timer

Beginning in privileged EXEC mode, follow these steps to configure the IGMP leave timer:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip igmp snooping last-member-query-interval** *time*	Configure the IGMP leave timer globally. The range is from 100 to 5000 milliseconds.
Step 3	**ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *time*	(Optional) Configure the IGMP leave timer on the VLAN interface. The range is from 100 to 5000 milliseconds. **Note** Configuring the leave time on a VLAN overrides the globally configured timer.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show ip igmp snooping**	(Optional) Display the configured IGMP leave time.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no ip igmp snooping last-member-query-interva**l global configuration command to globally reset the IGMP leave timer to the default setting (1000 milliseconds).

Use the **no ip igmp snooping vlan** *vlan-id* **last-member-query-interval** global configuration command to remove the configured IGMP leave-time setting from the specified VLAN.

For more information about commands that support the IGMP configurable leave time, see these sections:

- "ip igmp snooping last-member-query interval" section on page 32
- "show ip igmp snooping" section on page 33

QoS Updates

The default QoS egress queue settings for Queue 2 changed in Cisco IOS Release 12.2(25)SEB. These are the new settings for Queue 2:

Table 7 Default Egress Queue Configuration

Feature	Queue 1	Queue 2	Queue 3	Queue 4
Buffer allocation	25 percent	25 percent	25 percent	25 percent
WTD drop threshold 1	100 percent	200 percent	100 percent	100 percent
WTD drop threshold 2	100 percent	200 percent	100 percent	100 percent
Reserved threshold	50 percent	50 percent	50 percent	50 percent
Maximum threshold	400 percent	400 percent	400 percent	400 percent
SRR shaped weights (absolute) [1]	25	0	0	0
SRR shared weights [2]	25	25	25	25

1. A shaped weight of zero means that this queue is operating in shared mode.
2. One quarter of the bandwidth is allocated to each queue.

Updates to the Command Reference

These sections describe the commands that were added or updated in the command reference for this release:

- "clear port-security" section on page 30
- "ip igmp snooping last-member-query interval" section on page 32
- "show ip igmp snooping" section on page 33
- "switchport port-security" section on page 36
- "show version" section on page 36

clear port-security

Use the **clear port-security** privileged EXEC command on the switch stack or on a standalone switch to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

clear port-security {**all** | **configured** | **dynamic** | **sticky**} [[**address** *mac-addr* | **interface** *interface-id*] [**vlan** {*vlan-id* | {**access** | **voice**}}]]

Syntax Description

all	Delete all secure MAC addresses.
configured	Delete configured secure MAC addresses.
dynamic	Delete secure MAC addresses auto-learned by hardware.
sticky	Delete secure MAC addresses, either auto-learned or configured.
address *mac-addr*	(Optional) Delete the specified dynamic secure MAC address.
interface *interface-id*	(Optional) Delete all the dynamic secure MAC addresses on the specified physical port or VLAN.
vlan	(Optional) Delete the specified secure MAC address from the specified VLAN. Enter one of these options after you enter the **vlan** keyword: • *vlan-id*—On a trunk port, specify the VLAN ID of the VLAN on which this address should be cleared. • **access**—On an access port, clear the specified secure MAC address on the access VLAN. • **voice**—On an access port, clear the specified secure MAC address on the voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEA	This command was introduced.
12.2(25)SEB	The **access** and **voice** keywords were added.

Examples

This example shows how to clear all secure addresses from the MAC address table:

```
Switch# clear port-security all
```

This example shows how to remove a specific configured secure address from the MAC address table:

```
Switch# clear port-security configured address 0008.0070.0007
```

This example shows how to remove all the dynamic secure addresses learned on a specific interface:

```
Switch# clear port-security dynamic interface gigabitethernet1/0/1
```

This example shows how to remove all the dynamic secure addresses from the address table:

```
Switch# clear port-security dynamic
```

You can verify that the information was deleted by entering the **show port-security** privileged EXEC command.

Related Commands

Command	Description
switchport port-security	Enables port security on an interface.
switchport port-security mac-address *mac-address*	Configures secure MAC addresses.
switchport port-security maximum *value*	Configures a maximum number of secure MAC addresses on a secure interface.
show port-security	Displays the port security settings defined for an interface or for the switch.

ip igmp snooping last-member-query interval

Use the **ip igmp snooping last-member-query-interval** global configuration command to enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis. Use the **no** form of this command to return the IGMP configurable-leave timer to the default setting.

ip igmp snooping vlan *vlan-id* **last-member-query-interval** *time*

no ip igmp snooping vlan *vlan-id* **last-member-query-interval**

Syntax Description

vlan-id	(Optional) Specify a VLAN; the range is 1 to 4094 (available only in privileged EXEC mode).
time	Interval time out in seconds. The range is 100 to 5000 milliseconds.

Defaults

The default timeout setting is 1000 milliseconds.

Command History

Release	Modification
12.2(25)SEB	This command was introduced.

Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all the existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all the existing VLAN interfaces.

Configuring the leave timer on a VLAN overrides the global setting.

The IGMP configurable leave time is only supported on devices running IGMP Version 2.

The configuration is saved in NVRAM.

Examples

This example shows how to globally enable the IGMP leave timer for 2000 milliseconds:

```
Switch# configure terminal
Switch(config)# ip igmp snooping last-member-query-interval 2000
Switch(config)# end
```

This example shows how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:

```
Switch# configure terminal
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
Switch(config)# end
```

This example shows how to globally reset the IGMP leave timer to the default setting:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping last-member-query-interval
Switch(config)# end
```

This example shows how to remove the configured IGMP leave timer on VLAN 1. The globally configured leave timer is then applied to VLAN 1:

```
Switch# configure terminal
Switch(config)# no ip igmp snooping vlan 1 last-member-query-interval
Switch(config)# end
```

To verify your settings, enter the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping vlan	Enables IGMP snooping on a VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

show ip igmp snooping

Note Beginning with Cisco IOS Release 12.2(25)SEB, the value of the IGMP configurable-leave timer is displayed in the output of the **show ip igmp snooping** command.

Use the **show ip igmp snooping** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

groups	(Optional) See the **show ip igmp snooping groups** command.
mrouter	(Optional) See the **show ip igmp snooping mrouter** command.
querier	(Optional) Display the IP address and incoming port for the IGMP query most recently received by the switch.
vlan *vlan-id*	(Optional) Specify a VLAN; the range is 1 to 4094 (available only in privileged EXEC mode).
| **begin**	(Optional) Display begins with the line that matches the *expression*.
| **exclude**	(Optional) Display excludes lines that match the *expression*.

| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

The **vlan** *vlan-id* keyword is available only in privileged EXEC mode.

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.1(19)EA1	The **querier** keyword was added.
12.2(18)SE	The **groups** keyword was added. The **show ip igmp snooping groups** command replaced the **show ip igmp snooping multicast** command.

Usage Guidelines

Use this command to display snooping configuration for the switch or for a specific VLAN.

Although visible in the output display, output lines for topology change notification (TCN) and source-only learning are not valid.

Use the **show ip igmp snooping querier** command to display the IGMP version and IP address of a detected device that sends IGMP query messages, which is also called a *querier*. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router.* If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN.

This is an example of output from the **show ip igmp snooping** command:

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                       :Enabled
Immediate leave                     :Disabled
Multicast router learning mode      :pim-dvmrp
Source only learning age timer      :10
Last member query interval          :100
```

```
CGMP interoperability mode          :IGMP_ONLY

Vlan 2:
--------
IGMP snooping                       :Enabled
Immediate leave                     :Disabled
Multicast router learning mode      :pim-dvmrp
Source only learning age timer      :10
CGMP interoperability mode          :IGMP_ONLY
Last member query interval          : 333
<output truncated>
```

This is an example of output from the **show ip igmp snooping vlan 1** command:

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                       :Enabled
Immediate leave                     :Disabled
Multicast router learning mode      :pim-dvmrp
Source only learning age timer      :10
Last member query interval        : 100
CGMP interoperability mode          :IGMP_ONLY
```

This is an example of output from the **show ip igmp snooping mrouter vlan 1** command:

Note In this example, `Fa0/3` is a dynamically learned router port, and `Fa0/2` is a configured static router port.

```
Switch# show ip igmp snooping mrouter vlan 1
Vlan    ports
----    -----
   1    Fa0/2(static), Fa0/3(dynamic)
```

This is an example of output from the **show ip igmp snooping group vlan 1** command:

```
Switch# show ip igmp snooping group vlan 1
Vlan      Group          Version     Port List
---------------------------------------------------------
1         229.2.3.4      v3          fa0/1 fa0/3
1         224.1.1.1      v2          fa0/8
```

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
---------------------------------------------------
1         172.20.50.11   v3                  fa0/1
2         172.20.40.20   v2                  Router
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

show version

This note was added to the **show version** user EXEC command in the switch command reference:

Note Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

switchport port-security

Use the **switchport port-security** interface configuration command without keywords on the switch stack or on a standalone switch to enable port security on the interface. Use the keywords to configure secure MAC addresses, sticky MAC address learning, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default states.

switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

no switchport port-security [**mac-address** *mac-address* [**vlan** {*vlan-id* | {**access** | **voice**}}] | **mac-address sticky** [*mac-address* | **vlan** {*vlan-id* | {**access** | **voice**}}]] [**maximum** *value* [**vlan** {*vlan-list* | {**access** | **voice**}}]]

switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

no switchport port-security [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

Syntax Description

aging	(Optional) See the **switchport port-security aging** command.
mac-address *mac-address*	(Optional) Specify a secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.
vlan *vlan-id*	(Optional) On a trunk port only, specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.
vlan access	(Optional) On an access port only, specify the VLAN as an access VLAN.
vlan voice	(Optional) On an access port only, specify the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

mac-address sticky [*mac-address*]	(Optional) Enable the interface for *sticky learning* by entering only the **mac-address sticky** keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses. (Optional) Enter a *mac-address* to specify a sticky secure MAC address.
maximum *value*	(Optional) Set the maximum number of secure MAC addresses for the interface. The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. It is approximately 6000 for the Catalyst 2970 switches. For the Catalyst 3750 and 3560 switches, this number is determined by the active Switch Database Management (SDM) template. See the **sdm prefer** command. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces. The default setting is 1.
vlan [*vlan-list*]	(Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the **vlan** keyword is not entered, the default value is used. • **vlan**—set a per-VLAN maximum value. • **vlan** *vlan-list*—set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
violation	(Optional) Set the security violation mode or the action to be taken if port security is violated. The default is **shutdown**.
protect	Set the security violation protect mode. In this mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred. **Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

restrict	Set the security violation restrict mode. In this mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.
shutdown	Set the security violation shutdown mode. In this mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Defaults

The default is to disable port security.

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

The default violation mode is **shutdown**.

Sticky learning is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(25)SEB	The **access** and **voice** keywords were added.

Usage Guidelines

A secure port has these limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port. (Catalyst 3750 and 3560 only)
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot be a private-VLAN port. (Catalyst 3750 and 3560 only)
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP Phone, the Cisco IP Phone requires up to two MAC addresses. The Cisco IP Phone address is learned on the voice VLAN and might also be learned on the access VLAN. Connecting a PC to the Cisco IP Phone requires additional MAC addresses.

- Voice VLAN is supported only on access ports and not on trunk ports.
- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

If you enable port security on a voice VLAN port and if there is a PC connected to the IP phone, you should set the maximum allowed secure addresses on the port to more than 1.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause** *psecure-violation* global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration. If you remove the sticky MAC addresses from the running configuration, the sticky secure MAC addresses are removed from the running configuration and the address table.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky** *mac-address* interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky** *mac-address* interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

Examples

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

This example shows how to configure a secure MAC address and a VLAN ID on a port.

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

You can verify your settings by using the **show port-security** privileged EXEC command.

Related Commands

Command	Description
clear port-security	Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface.
show port-security address	Displays all the secure addresses configured on the switch.
show port-security interface *interface-id*	Displays port security configuration for the switch or for the specified interface.

Related Documentation

These documents provide complete information about the Cisco EtherSwitch service modules and are available on Cisco.com:

- *Cisco EtherSwitch Service Modules (NME-16ES-1G-P, NME-X-23ES-1G-P, NME-XD-48ES-2S-P, NME-XD-24ES-1S-P)*
- *Cisco Network Modules Hardware Installation Guide*
- *Cisco 3800 Series Hardware Installation*
- *Cisco 2800 Series and Cisco 3800 Series Integrated Services Routers Regulatory Compliance and Safety Information*

For information about related products, see these documents:

- *Catalyst 3750 Switch Software Configuration Guide* (order number DOC-7816180=)
- *Catalyst 3750 Switch Command Reference* (order number DOC-7816181=)
- *Catalyst 3750 Switch System Message Guide* (order number DOC-7816184=)
- *Catalyst 3750 Switch System Message Guide* (order number DOC-7816184=)
- Device manager online help (available on the switch)
- *Catalyst 3750 Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750 Switch Getting Started Guide (*order number DOC-7816663=)
- *Regulatory Compliance and Safety Information for the Catalyst 3750 Switch* (order number DOC-7816664)
- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)

Obtaining Documentation

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

Cisco.com

You can access the most current Cisco documentation at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

- 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 1 800 553-NETS (6387).

Documentation Feedback

You can send 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

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

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—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.

Severity 2 (S2)—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.

Severity 3 (S3)—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.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

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

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

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

  http://www.cisco.com/ipj
- World-class networking training is available from Cisco. You can view current offerings 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.