



Release Notes for the Cisco ME 2400 Ethernet Access Switches, Cisco IOS Release 12.2(25)EX and Later

Revised January 31, 2007

These release notes include important information about Cisco IOS Release 12.2(25)EX and Cisco IOS Release 12.2(25)EX1, and any limitations, restrictions, and caveats that apply to the releases. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the “[Finding the Software Version and Feature Set](#)” section on page 3.
- 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 3.

For the complete list of Cisco ME 2400 switch documentation, see the “[Related Documentation](#)” section on page 16.

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

<http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi>

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

Cisco IOS Release 12.2(25)EX and later are based on Cisco IOS Release 12.2(25)SEB4. Open caveats in Cisco IOS Release 12.2(25)SEB4 also affect this release, unless they are listed in the resolved caveats list in these release notes. The list of open caveats in Cisco IOS Release 12.2(25)SEB4 is available at this URL:

http://www.cisco.com/en/US/products/hw/switches/ps5023/prod_release_note09186a008041a334.html



Corporate Headquarters:

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

© 2005 Cisco Systems, Inc. All rights reserved.

Contents

This information is in the release notes:

- [“System Requirements” section on page 2](#)
- [“Upgrading the Switch Software” section on page 3](#)
- [“Installation Notes” section on page 5](#)
- [“New Features” section on page 6](#)
- [“Limitations and Restrictions” section on page 6](#)
- [“Open Caveats” section on page 9](#)
- [“Resolved Caveats” section on page 14](#)
- [“Documentation Updates” section on page 15](#)
- [“Related Documentation” section on page 16](#)
- [“Obtaining Documentation” section on page 16](#)
- [“Documentation Feedback” section on page 17](#)
- [“Cisco Product Security Overview” section on page 18](#)
- [“Obtaining Technical Assistance” section on page 19](#)
- [“Obtaining Additional Publications and Information” section on page 20](#)

System Requirements

The system requirements are described in this section:

- [“Hardware Supported” section on page 2](#)

Hardware Supported

[Table 1](#) lists the hardware supported on Cisco IOS Release 12.2(25)EX.

Table 1 **Supported Hardware**

Device	Description
ME-2400-24TS-A	24 10/100 ports and 2 SFP module slots, AC power
ME-2400-24TS-D	24 10/100 ports and 2 SFP module slots, DC power
SFP modules	1000BASE-T, -BX, -SX, -LX/LH, -ZX 100BASE-BX, FX, -LX Coarse wavelength-division multiplexing (CWDM)
Cable	Catalyst 3650 SFP interconnect cable

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 3](#)
- [“Deciding Which Files to Use” section on page 3](#)
- [“Archiving Software Images” section on page 3](#)
- [“Upgrading a Switch by Using the CLI” section on page 4](#)
- [“Recovering from a Software Failure” section on page 5](#)

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. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

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

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

[Table 2](#) lists the filenames for this software release.

Table 2 Cisco IOS Software Image Files

Filename	Description
me240x-metrobase-tar.122-25.EX1.tar	Cisco ME 2400 metro base image. This image has basic Metro Ethernet features.
me240x-metrobasek9-tar.122-25.EX1.tar	Cisco ME 2400 metro base cryptographic image. This image has the Kerberos, Secure Shell (SSH), and basic Metro Ethernet features.

Archiving Software Images

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

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

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

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the “Basic File Transfer Services Commands” section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/ffrprt2/frf011.htm#wp1018426

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.



Note

For downloading software, we recommend that you connect to the TFTP server through a network node interface (NNI). If you want to connect to the server through a user network interface (UNI), see the “Troubleshooting” chapter of the software configuration guide for methods for enabling ping capability on UNIs. See the “[New Software Features](#)” section on page 6 for a definition of NNIs and UNIs.

To download software, follow these steps:

-
- Step 1** Use [Table 2 on page 3](#) to identify the file that you want to download.
- Step 2** Download the software image file. If you have a SmartNet support contract, log in to cisco.com and go to this URL, and log in to download the appropriate files:
- <http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi>
- Click on “*Launch the IOS Upgrade Planner*” and search for ME 2400 to download the appropriate files:
- To download the image for a Cisco ME 2400 switch, click **Cisco ME 2400 software**.
 - To obtain authorization and to download the cryptographic software files, click **Cisco ME 2400 3DES Cryptographic Software**.
- Step 3** Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.
- For more information, refer to Appendix B in the software configuration guide for this release.
- Step 4** Log into the switch through the console port or a Telnet session.
- Step 5** (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:
- ```
Switch# ping tftp-server-address
```

**Note**

By default, ping is supported on network node interfaces (NNIs), but you cannot ping from a user network interface (UNI) because the control-plane security feature drops ICMP response packets received on UNIs. See the “Troubleshooting” chapter of the software configuration guide for methods for pinging from the switch to a host connected to a UNI. See the “[New Software Features](#)” section on page 6 for a definition of NNIs and UNIs.

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/me240x-metrobase-tar.122.25.EX.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 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 6](#)
- [“New Software Features” section on page 6](#)

## New Hardware Features

For a list of all supported hardware, see the [“Hardware Supported” section on page 2](#).

## New Software Features

This release is the first software release for the Cisco ME switch, which introduces several features specifically designed for service-provider networks:

- The Cisco ME switch has two different types of interfaces: network node interfaces (NNIs) to connect to the service provider network and user network interfaces (UNIs) to connect to customer networks. Some features are supported only on one of these port types. By default, the 10/100 ports on the switch are configured as UNIs, and the SFP module uplink ports are configured as NNIs. However, you can configure up to four NNIs on each switch. See the “Configuring Interface Characteristics” chapter of the software configuration guide for details.
- UNI-isolated VLANs isolate customer VLANs from VLANs of other customers on the same switch. Local switching does not occur among UNIs on the switch that belong to the same UNI isolated VLAN. See the “Configuring VLANs” chapter of the software configuration guide for details.
- Automatic control-plane security protects the CPU from accidental or malicious overload due to Layer 2 control traffic on UNIs. See the “Configuring Control Plane Security” chapter of the software configuration guide for details.

For a detailed list of key features for this software release, refer to the “Overview” chapter of the software configuration guide for this release.

## Limitations and Restrictions

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

These limitations apply to the Cisco ME switches:

- [“Configuration” section on page 7](#)
- [“SPAN and RSPAN” section on page 8](#)
- [“Trunking” section on page 8](#)
- [“VLAN” section on page 8](#)

## 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)

- 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 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)
- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW\_NEW\_SOURCE record is before the BLOCK\_OLD\_SOURCE record, the switch removes the port from the group.
  - If the BLOCK\_OLD\_SOURCE record is before the ALLOW\_NEW\_SOURCE record, the switch adds the port to the group.

There is no workaround. (CSCec20128)

- 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)

## SPAN and RSPAN

This is the SPAN limitation:

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

## Trunking

These are the trunking limitations:

- Trunk port that belong to the same community VLAN cannot switch traffic. See the “Configuring VLANs” chapter of the software configuration guide for information about community and isolated VLANs.
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).
- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

## VLAN

These are the VLAN limitations:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 5,000, the switch can fail.

The workaround is to not configure more than the recommended number of VLANs and 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)

# Open Caveats

This section describes the open caveats with possible unexpected activity in this software release.

- 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 switch 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.

- CSCeh54035

When IGMP snooping is disabled on the switch, CPU control-plane security does not prevent IGMP packets received on UNI ports from being sent to the CPU.

The workaround is to not disable IGMP snooping if you want CPU control-plane security to be in effect for IGMP packets.

- CSCsb69014

When you enter the **flash\_init** boot loader command to initialize the flash file system on the switch, the command might not work the first time that you enter it.

The workaround, if you encounter any problems accessing the flash partition, is to enter the **flash\_init** boot loader command again.

- CSCsb69676

When individual policing or aggregate policing is configured in a policy map with the policing exceed-action based on table-maps, after the policy is attached to an interface you cannot overwrite the configuration with a new police exceed-action based on a different table map.

- For example, when a policy map with an individual policer is attached to an interface and you enter the **police** *{rate-bps | cir cir-bps}* **exceed action set-dscp-transmit dscp table** *policed-table-map name* policy-map class configuration command, the switch does not allow the configured table-map name to be overwritten with the new policed table-map name.
- Similarly, when a policy map using an aggregate policer is attached to an interface and you enter the **policer aggregate** *aggregate-policer-name* *{rate-bps | cir cir-bps}* **exceed action set-dscp-transmit dscp table** *table-map name* global configuration command, the switch does not allow the configured table-map name to be overwritten with the new table-map name.

These are the workarounds if you need to change the table-map name for the two different kinds of policing actions, using the same examples shown in the previous paragraphs.

For a policy map configured for individual policing:

1. Delete the current exceed-action by entering the **no police** *{rate-bps | cir cir-bps}* **exceed action set-dscp-transmit dscp table** *policed-table-map name* command (with the current table map name).
2. Configure the exceed-action marking with the new table-map name by entering the **police** *{rate-bps | cir cir-bps}* **exceed action set-dscp-transmit dscp table** *policed-table-map name* command (with the new table map name).

For a policy map configured globally for aggregate policing:

1. Change the exceed action to **drop** by entering the **policer aggregate** *aggregate-policer-name* *{rate-bps | cir cir-bps}* **exceed action drop** command.
2. Configure the exceed-action marking with the new table-map name by entering the **policer aggregate** *aggregate-policer-name* *{rate-bps | cir cir-bps}* **exceed action set-dscp-transmit dscp table** *table-map name* command (with the new table map name).

- CSCsb74505

When you are removing a CNS configuration by entering the **no cns config initial** *host port-number* global configuration command, the configuration is correctly removed, but this message might be displayed:

```
%CNS-3-TRANSPORT: Error=[CNS_HTTP_CONNECTION_FAILED] Root Tag=[ROOT_TAG_NA] Child Tag=[CHILD_TAG_NA] -Process= "CNS config initial", ipl= 0, pid= 3
```

There is no known workaround.

- CSCsb74925

When you are configuring a large number of ports as SPAN destination ports, this message might appear:

```
%SYS-3-CPUHOG: Task is running for (2097)msecs, more than (2000)msecs (0/0), process = Exec. -Traceback= B394 22ABE4 22AE0C 2FCF24 2F7D78 41023C 904E0 418EC4 4026A4 77CE8C 77D648 77DB30 77E558 781EE0 7741FC 7746CC
```

There is no workaround. The message is not correct; the ports are configured according to the entered commands.

- CSCsb86336

If you try to enter the **bandwidth remaining percent** *value* policy-map class configuration command and the **bandwidth percent** *value* policy-map class configuration command in the same policy map, the configuration is not allowed and the error message that appears is misleading:

```
All class bandwidths have to be consistently in kbps or percentage
```

The workaround is to not use the **bandwidth percent** *value* command and the **bandwidth remaining percent** *value* command in the same policy map. This is an invalid configuration.

- CSCsb98219

When you use the **bandwidth** policy-map class command to configure more than one class in a policy map for Class-based Weighted Fair Queuing (CBWFQ), and the committed information rate (CIR) bandwidth for any of the classes is less than 2 percent of the interface rate, the CBWFQ classes in the policy map may not receive the configured CIR bandwidths.

There is no workaround, but it is unlikely that a CBWFQ class would be configured with such a low CIR bandwidth.

- CSCsc14748

When a port belongs to a private VLAN primary VLAN and also belongs to VLAN 1, deleting the primary VLAN might also shut down the line protocol for that port's switch virtual interface (SVI) on VLAN 1. This can occur when several ports, in addition to the one belonging to the primary VLAN, also belong to VLAN 1.

There is no workaround.

- CSCsc16012

When you use the **bandwidth percent** policy-map class command to configure a class in a policy map, attach the policy map to an interface, and configure the same policy map as a child policy to a parent port-shaping policy map that is also attached to an interface, the **show policy-map interface interface-id** user EXEC command for the latter interface does not show the correct bandwidth for the class configured with the **bandwidth percent** command. It displays an incorrect equivalent absolute bandwidth in bps for the class as a percentage of the interface rate, instead of a percentage of the configured port-shape rate.

There is no workaround. This is a display-only problem that only occurs in this specific situation. The functionality works correctly.

- CSCsc17257

When you configure an input policy map that uses a table map to map an incoming CoS (IEEE 801.1p bit) value (*from cos*) to another packet marking and you try to attach it to a port that is incapable of receiving IEEE 802.1Q or IEEE 8023.1p tagged packets, the switch incorrectly allows you to do so. The problem can occur when you attach the policy map to a non-trunk interface by entering the **service-policy input policy-map-name** interface configuration command, attach the policy map to a trunk interface and change the interface to a non-trunk interface, or attach another valid policy map to a non-trunk interface and the policy map is dynamically changed to a *from-cos* table map.

The workaround is to not attach a policy map with a *from-cos* based table-map action to a non-trunk interface.

- CSCsc20515

If you create a private VLAN domain with a primary and secondary VLAN, configure the secondary VLAN as a community VLAN, and then use the **switchport private-vlan host** and **switchport private-vlan host-association** interface configuration commands to associate ports to the private VLAN, the LEDs on the ports that belong to the secondary VLAN display as amber. However, if you then use the **monitor session session\_number destination interface interface-id** global configuration command for one of these ports to configure it as a SPAN destination port and later configure it again as a member of the secondary community VLAN, the LED changes to green.

The workaround is to use the **shutdown** and then **no shutdown** interface configuration commands on the interface. The change of state from down to up results in the interface correctly showing as amber.

- CSCsc21602

You cannot attach an output policy-map that has a class associated with qualified queue-limit to an interface when all queue-limit qualifiers are correctly represented by the associated class-map classification criteria, but the class map has one or more classification criteria that are not represented by any queue-limit qualifiers. This error message appears even when the condition mentioned in the message is satisfied:

```
QoS: Configuration failed. All queue-limit qualifier criteria must be represented
within the associated class-map classification criteria
```



**Note**

A *qualified queue limit* is when you configure a different queue limit for one or more different classification criteria of the class map, for example by entering the command **queue-limit dscp 30 48**.

The same error message appears when a policy map with a qualified queue-limit is attached to an interface and a class-map classification criteria not associated with any configured queue-limit qualifier is added to the class map associated with qualified queue-limit. In this case, in spite of the error message, the configuration is accepted.

The same error message also appears when a policy-map with qualified queue-limit is attached to an interface and a class-map classification criteria already associated with a configured queue-limit qualifier is deleted from the class map associated with qualified queue-limit. In this case also, in spite of the error message, the configuration is accepted.

The workaround is when you configure an output policy-map with qualified queue-limit, you should ensure that each classification criteria in the class-map associated with qualified queue-limit is represented by a unique qualified queue-limit. The threshold value to which each queue-limit qualifier is mapped is flexible and based on requirements.

In the cases in which the configuration is accepted even after the error message is displayed, you can ignore the error message.

- CSCsc24495

A policy map with CoS-based classification is not valid on a non-trunk interface, and the switch does not allow you to attach it. However, when an output hierarchical port-shaping policy map with a child policy that has CoS classification is attached to a trunk interface and the interface is later changed to a non-trunk interface, the policy map is not detached as it should be. This is not a problem with any other kind of policy. For example if a non-hierarchical output policy map with CoS-based classification is attached to a trunk interface, and the interface is changed to a non-trunk interface, the policy is correctly detached.

The workaround is to not attach a policy map with CoS-based classification to a non-trunk interface. If you attach such a policy to a trunk interface and later use the **switchport mode** interface configuration command to change the interface to a non-trunk interface, you should detach the policy before changing the port mode.

- CSCsc26465

When a CWDM-type SFP module is installed in the switch, the CWDM device is not listed in the output of the **show inventory** User EXEC command.

The workaround is to use the **show inventory raw** User EXEC command. to see a listing of all entities in the switch.

- CSCsc30193

When you configure an input policy-map with a **set** action that references an invalid table map, the configuration is correctly rejected with an error message. A table map is invalid for a **set** action when the value of the *from-* or *to-* type parameter of the table map is inconsistent with the *from-* or *to-* type specified in the **set** action. However, after the configuration is rejected, if no other valid action is configured for that class, packets might be incorrectly marked for that class.

The workaround is to not try to configure an invalid or inconsistent table map for a set action. If one is incorrectly configured, configure the action for that class to any other valid action.

- CSCsc30194

When one output policy map (*policy-map1*) that is attached to an interface has a class configured for an unqualified queue-limit or no queue-limit at all, and another output policy map (*policy-map2*) attached to an interface has a qualified queue limit configured for the same class, if *policy-map1* is *detached* from the interface before you detach *policy-map2*, an incorrect queue limit might be applied to some packets in the class.

**Note**


---

An *unqualified queue limit* is a single queue limit that applies to all the classification criteria of the class map, configured by entering the **queue-limit number-of-packets** policy-map class command.

A *qualified queue limit* is when you configure a different queue limit for one or more different classification criteria of the class map, for example by entering the command **queue-limit dscp 30 48**.

---

The queue-limit applied for packets that match the specified class is not the qualified queue-limit value specified in *policy-map2*, but either the user-configured unqualified queue-limit value for that class (specified in *policy-map2*) or if no unqualified queue limit was configured for the class in *policy-map2*, the default value of 48 packets. Packets that belong to other classes get the expected treatment.

The workaround is that whenever you configure an output policy map with a qualified queue-limit for a class, you should be sure that all other output policy maps attached to any interface also contain the same qualified queue-limit for that class. However, the configured qualified queue-limit values can be different values in the different policy maps.

- CSCsc30211

When an output policy map (*policy-map1*) that has a class configured for an unqualified queue-limit is *attached* to an interface before another output policy map (*policy-map2*) that has a qualified queue limit configured for the same class is attached to an interface, the queue limit applied for some packets matching the specified class for *policy map1* will be the default value of 48 packets, instead of the user-configured unqualified queue-limit value.

**Note**


---

An *unqualified queue limit* is a single queue limit that applies to all the classification criteria of the class map, configured by entering the **queue-limit number-of-packets** policy-map class command.

A *qualified queue limit* is when you configure a different queue limit for one or more different classification criteria of the class map, for example by entering the command **queue-limit dscp 30 48**.

---

This happens only for packets that match the classification criteria for which the qualified queue-limit is specified in output *policy-map-2*. The rest of the packets will get the expected treatment.

The workaround is that whenever you configure an output policy map with a qualified queue-limit for a class, you should be sure that all other output policy maps attached to any interface also contain the same qualified queue-limit for that class. However, the configured qualified queue-limit values can be different values in the different policy maps.

- CSCsc35915

Although the documentation says that you can configure 48 policers per port and 229 policers per switch, you can configure only 47 policers on a port and 228 on the switch. One less policer can be configured per-port and per switch than is documented.

There is no workaround. Do not attempt to configure more than 47 policers per port or 228 per switch.

## Resolved Caveats

These are the caveats that have been resolved in these releases.

- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)EX1” section on page 14](#)
- [“Resolved IOS Caveats in Cisco IOS Release 12.2\(25\)EX” section on page 15](#)

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)EX1

These caveats were resolved in Cisco IOS Release 12.2(25)EX1:

- CSCek26492

Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

- CSCek37177

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

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

This issue is documented as Cisco bug ID CSCek37177.

There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

- CSCse08786

This DDTS documents changes in how IOS handles packets destined to the router or switch.

## Resolved IOS Caveats in Cisco IOS Release 12.2(25)EX

This caveat was resolved in Cisco IOS Release 12.2(25)EX:

- CSCei54611

**Symptoms:** The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

**Conditions:** The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

**Further Information:** On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at <http://www.cisco.com/warp/public/707/cisco-sr-20060913-vtp.shtml>

- CSCei61732

Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

Cisco has made free software available that includes the additional integrity checks for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.

## Documentation Updates

### Correction to the Getting Started Guide

In Step 5 of the “Initial Setup” section, the maximum power consumption is listed as 40 W. The correct maximum power consumption is 30 W.

## Related Documentation

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

<http://www.cisco.com/univercd/cc/td/doc/product/metro/me2400/index.htm>

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the “[Obtaining Documentation](#)” section on page 16.

- *Cisco ME 2400 Ethernet Access Switch Software Configuration Guide* (order number DOC-7817059=)
- *Cisco ME 2400 Ethernet Access Switch Command Reference* (order number DOC-7817061=)
- *Cisco ME 2400 Ethernet Access Switch System Message Guide* (order number DOC-7817063=)
- *Cisco ME 2400 Ethernet Access Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Cisco ME 3400 and ME 2400 Ethernet Access Switches Getting Started Guide* (order number DOC-7817050=)
- *Regulatory Compliance and Safety Information for the Cisco ME 3400 and ME 2400 Ethernet Access Switches* (order number DOC-7817051)
- *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)
- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco CWDM SFP Transceiver Compatibility Matrix* (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/techsupport>

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](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto: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](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](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](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

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

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



**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 linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation 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, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation 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 & Documentation 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 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 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, documentation, 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>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *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>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- 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.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)

© 2005-6 Cisco Systems, Inc. All rights reserved.

