Release Notes for the Cisco ME 3400E and ME 3400 Ethernet Access Switches, Cisco IOS Release 12.2(54)SE

April 20, 2010

Cisco IOS Release 12.2(54)SE runs on the Cisco ME 3400E and ME 3400 Series Ethernet Access switches.

These release notes include important information about Cisco IOS Release 12.2(54)SE and any limitations, restrictions, and caveats that apply to the release. 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 or different image, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 4.

For the complete list of Cisco ME 3400E and ME 3400 switch documentation, see the "Related Documentation" section on page 39.

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

http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches

Contents

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

Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2(50)SE.

Table 1 Supported Hardware

Device	Description	Supported by Minimum Cisco IOS Release
ME 3400E-24TS-M	24 10/100 ports and 2 dual-purpose ports; supports removable AC- and DC-power supplies.	Cisco IOS Release 12.2(44)EY
ME 3400EG-12CS-M	12 dual-purpose ports and 4 SFP module slots; supports removable AC- and DC-power supplies.	Cisco IOS Release 12.2(44)EY
ME 3400EG-2CS-A	2 dual-purpose ports and 2 SFP module slots, AC-power input.	Cisco IOS Release 12.2(44)EY
ME 3400-24FS-A	24 100BASE-FX SFP module ports and 2 Gigabit Ethernet SFP module ports, AC power	Cisco IOS Release 12.2(40)SE
ME 3400G-2CS	2 dual-purpose ports and 2 SFP-only module ports, AC power	Cisco IOS Release 12.2(35)SE1
ME-3400G-12CS-A	12 dual-purpose ports and 4 SFP-only module ports	Cisco IOS Release 12.2(25)SEG1
ME-3400G-12CS-D	12 dual-purpose ports and 4 SFP-only module ports	Cisco IOS Release 12.2(25)SEG1
ME-3400-24TS-A	24 10/100 ports and 2 SFP module slots, AC power	Cisco IOS Release 12.2(25)EX
ME-3400-24TS-D	24 10/100 ports and 2 SFP module slots, DC power	Cisco IOS Release 12.2(25)EX
SFP modules ME 3400	1000BASE-T, -BX, -SX, -LX/LH, -ZX 100BASE-BX, FX, -LX Coarse wavelength-division multiplexing (CWDM)	Cisco IOS Release 12.2(25)EX
	Digital optical monitoring (DOM) support for GLC-BX, CWDM and DWDM SFPs	Cisco IOS Release 12.2(44)SE
	100BASE-EX, 100BASE-ZX 1000BASE-LX/LH MMF and SMF 1000BASE-SX MMF DOM support for GLC-ZX-SM SFP, 1000BASE-LX/LH, and 1000BASE-SX	Cisco IOS Release 12.2(46)SE
	DOM support for 1000BASE-BX Additional DWDM SFPs qualification	Cisco IOS Release 12.2(50)SE

For a complete list of ME 3400 supported SFPs and part numbers, see the ME 3400 data sheet at:

http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps6580/product_data_sheet0900aecd8034fef3.html

Table 1 Supported Hardware (continued)

Device	Description	Supported by Minimum Cisco IOS Release
SFP modules ME 3400E	1000BASE-BX10, -SX, -LX/LH, -ZX 100BASE -BX10, -EX, -FX (GLC-FE-100FX only), -LX10, -ZX 1000BASE-T and 10/100/100BASE-T—Category 5,6 (SFP-only ports; not supported on dual-purpose ports) Coarse wavelength-division multiplexing (CWDM) Dense wavelength-division multiplexing (DWDM) Digital optical monitoring (DOM) support for SFP-GE-S, SFP-GE-L, 1000BASE-BX10, 1000BASE-ZX, CWDM and DWDM SFPs **Note** See the hardware installation guide for SFP model numbers.	Cisco IOS Release 12.2(44)EY
	Additional DWDM SFPs qualification	Cisco IOS Release 12.2(50)SE
For a complete list of ME 3400E supported SFPs and part numbers, see the ME 3400E data sheet at: http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps9637/data_sheet_c78-495220.html		
Cable	Catalyst 3560 SFP interconnect cable	Cisco IOS Release 12.2(25)EX

Upgrading the Switch Software

Before downloading software, read this section for important information:

- Finding the Software Version and Feature Set, page 3
- Deciding Which Files to Use, page 4
- Archiving Software Images, page 4
- Upgrading a Switch, page 4
- Recovering from a Software Failure, page 6

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.

Note The ME 3400 metro base image is not supported on the Cisco ME 3400E switch.

Table 2 Cisco IOS Software Image Files

Filename	Description
me340x-metrobasek9-tar.122-54.SE.tar	Cisco ME 3400 metro base cryptographic image. This image has the Kerberos, Secure Shell (SSH), and basic Metro Ethernet features.
me340x-metroaccessk9-tar.122-54.SE.tar	Cisco ME 3400E and ME 3400 metro access cryptographic image. This image has the Kerberos, SSH, and Layer 2 + Metro Ethernet features.
me340x-metroipaccess9-tar.122-54.SE.tar	Cisco ME 3400E and ME 3400 metro IP access cryptographic image. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 routing 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/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.html#wp1018426

Upgrading a Switch

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 4 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 the ME3400 platform to select the appropriate files:

- Select the software release and image you want to download.
- You might need to obtain authorization and to download the cryptographic software files

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.

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/image-name.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by using the **/leave-old-sw** option instead of the **/overwrite** 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 these methods:

- Using the CLI-based setup program, as described in the switch hardware installation guide.
- Using 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

- New Hardware Features, page 6
- New Software Features, page 6

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

- Support for the IEEE 802.1ad standard to provide VLAN scalability in provider networks, giving provider bridges the same functionality as Layer 2 protocol tunneling (L2PT) and QinQ bridges. See the "Configuring IEEE 802.1ad" section on page 20 and "Updates to the ME 3400E Command Reference - Release 12.2(54)SE" section on page 30. (ME 3400E only)
- CFM support on a customer VLAN (C-VLAN), which allows a customer to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on a C-VLAN component to provide a customer with visibility to network traffic on the C-VLAN. See the "Configuring CFM on C-VLAN (Inner VLAN)" section on page 25.

- Support for the IEEE CFM (IEEE 802.1ap) MIB, which can be used as a tool to trace paths, to verify and to manage connectivity, and to detect faults in a network. See the ""Supported MIBs" Appendix" section on page 26.
- There is no limit to the number of times that you can enter the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command. You can block an unlimited number, range, or sequence of VLANs. (CSCta48811)
- For the product identifier (PID) and version identifier (VID) of small form-factor pluggable (SFP) modules, the output of the **show inventory** user EXEC command displays either the correct information or Unspecified for the PID and nothing for the VID if the SFP does not have PID and VID information. (CSCsu60206)
- There is no longer a restriction to the number of user network interfaces (UNIs) and enhanced network interfaces (ENIs) that you can add to a community VLAN or private VLAN. (CSCtc45248)

Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release (after the first release) required to support the features of the Cisco ME 3400E and ME 3400 switch. Features not listed are supported in all releases.

Note The first release for the Cisco ME3400E switch was 12.2(44)EY and it included all ME 3400 features through release 12.2(44)SE.

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
Support for the IEEE 802.1ad standard (ME 3400E).	12.2(54)SE
CFM support on customer VLANs (C-VLANs).	12.2(54)SE
IEEE CFM MIB support.	12.2(54)SE
Ingress QoS classification enhancements	12.2(53)SE
Support for ingress QoS classification on QinQ-based ports (ME 3400E).	12.2(53)SE
Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table.	12.2(52)SE
Support for IP source guard on static hosts.	12.2(52)SE
IEEE 802.1x user distribution for deployments with multiple VLANs (for a group of users) to improve network scalability by load balancing users across different VLANs. The RADIUS server assigns authorized users to the least populated VLAN in the group.	12.2(52)SE
Support for Network Edge Access Topology (NEAT) for changing the port host mode and applying a standard port configuration to the authenticator switch port.	12.2(52)SE
Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms.	12.2(52)SE
Support for including a hostname in the option 12 field of DHCPDISCOVER packets. Identical configuration files can be sent by using DHCP.	12.2(52)SE

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
DHCP snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE
Connectivity fault management (CFM) Draft 8.1 compliance to bring the OAM implementation up to the new IEEE standard.	12.2(52)SE
Support for the TWAMP standard for measuring round-trip network performance between any two devices that support the protocol.	12.2(52)SE
Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping.	12.2(52)SE
Support for QoS marking of CPU-generated traffic and queue CPU-generated traffic on the egress network ports.	12.2(52)SE
Multicast VLAN registration (MVR) enhancements include the ability to configure 2000 MVR groups when the switch is in dynamic MVR mode and a new command (**mvr ringmode flood**) to ensure that forwarding in a ring topology is limited to member ports.	12.2(52)SE
Shorter Resilient Ethernet Protocol (REP) hello: Changes the range of the REP link status layer (LSL) age timer from 3000 to 10000 ms in 500-ms intervals to 120 to 10000 ms in 40-ms intervals.	12.2(52)SE
Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.	12.2(52)SE
IPv6 routing support (metro IP access image only)	12.2(50)SE
IPv6 ACLs (metro IP access image only)	12.2(50)SE
BFD (metro IP access image only)	12.2(50)SE
REP support on ports connected to nonREP ports	12.2(50)SE
NEAT with 802.1X switch supplicant, host authorization with CISP, and auto enablement	12.2(50)SE
CPU utilization threshold trap	12.2(50)SE
EEM 2.4 (metro access image only on ME 3400)	12.2(50)SE
RADIUS server load balancing	12.2(50)SE
IP source guard in metro base image (ME 3400)	12.2(50)SE
Dynamic ARP inspection in metro base image (ME 3400)	12.2(50)SE
EOT and IP SLAs EOT static route support	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)
REP counter and timer enhancements	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)
HSRPv2 (metro IP access image only)	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)
DHCP server port-based address allocation	12.2(46)SE (ME 3400) 12.2(50)SE (ME 3400E)
DHCP-based autoconfiguration and image update	12.2(44)SE
Configurable small-frame arrival threshold	12.2(44)SE
Source Specific Multicast (SSM) mapping for multicast applications	12.2(44)SE

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
Support for the *, *ip-address*, **interface** *interface-id,* and **vlan** *vlan-id* keywords with the **clear ip dhcp snooping** command	12.2(44)SE
Flex Link Multicast Fast Convergence	12.2(44)SE
IEEE 802.1x readiness check	12.2(44)SE
Configurable control-plane queue assignment	12.2(44)SE
Configurable control plane security (support for ENIs)	12.2(44)SE
/31 bit mask support for multicast traffic	12.2(44)SE
Configuration rollback and replacement	12.2(40)SE
EEM (metro IP access image only) **Note** EEM support was added to the metro access image in 12.2(44)SE	12.2(40)SE
IGMP Helper (metro IP access image only)	12.2(40)SE
IP SLAs support (metro IP access and metro access images only)	12.2(40)SE
IP SLAs enhanced object tracking (metro IP access and metro access images only)	12.2(40)SE
IP SLAs for Ethernet OAM (metro IP access image only)	12.2(40)SE
Multicast VRF Lite (metro IP access image only)	12.2(40)SE
SSM PIM (metro IP access image only)	12.2(40)SE
REP (metro IP access and metro access images only)	12.2(40)SE
LLDP-MED location TLV (metro IP access and metro access images only)	12.2(40)SE
ELMI-CE	12.2(37)SE
LLDP and LLDP-MED	12.2(37)SE
Port security on a PVLAN host	12.2(37)SE
VLAN Flex Links load balancing	12.2(37)SE
Support for Multicast VLAN Registration (MVR) over trunk ports	12.2(35)SE1
Enhanced object tracking for HSRP (metro IP access image only)	12.2(35)SE1
Ethernet OAM IEEE 802.3ah protocol (metro IP access and metro access images only)	12.2(35)SE1
Ethernet OAM CFM (IEEE 802.1ag) and E-LMI (metro IP access and metro access images only)	12.2(25)SEG
Per port per VLAN QoS (metro IP access and metro access images only)	12.2(25)SEG
Support for all OSPF network types (metro IP access only)	12.2(25)SEG
Layer 2 protocol tunneling on trunks (metro IP access and metro access images only)	12.2(25)SEG
IS-IS protocol (metro IP access only)	12.2(25)SEG
NNIs on all ports (metro IP access image only)	12.2(25)SEG
DHCP server	12.2(25)SEG
DHCP Option-82 configurable remote ID and circuit ID	12.2(25)SEG
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEG
Nonstop forwarding (NSF) awareness (metro IP access image only)	12.2(25)SEG

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
Secure Copy Protocol	12.2(25)SEG
Flex Links sub-100-ms convergence; preemptive changeover (metro IP access and metro access images)	12.2(25)SEG
Link-state tracking (trunk failover) (metro IP access and metro access images only)	12.2(25)SEG

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.

Bidirectional Forwarding Detection

- The BFD session with the neighbor flaps when there is close to 100 percent bidirectional line- rate traffic sent through the physical links connecting the neighbors. This happens only on the sessions with Layer 3 BFD neighboring switches connected through a Layer 2 intermediate switch.

  The workaround is to make sure that there is no 100 percent bidirectional unknown traffic flowing through the intermediate Layer 2 switch in the same links that connect Layer 3 switches. An alternate workaround is to always directly the Layer 3 switches when BFD is running. (CSCsu94835)

- If you create a BFD session between two switches and then create an ACL that includes the **permit ip any any log-input** access-list configuration command, when you attach the ACL to one of the connecting interfaces, the BFD session goes down. If you remove the ACL from the interface, BFD comes back up.

  The workaround is to not use the **permit** ACL entry with the log option on interfaces participating in BFD. (CSCtf31731)

Connectivity Fault Management (CFM)

- On a switch running CFM, continuity check messages (CCMs) received on a MEP port that are a lower level than the configured MEP level should be discarded and an error message generated, regardless of whether or not the CCM has a valid CFM multicast destination address. On the ME 3400 switch, CFM C-VLAN CCMs with non-CFM multicast addresses are forwarded without CFM processing and no error messages are sent.

  There is no workaround. (CSCte39713)

- When the CFM start delay timer is configured to a small value, the *Crosscheck-Up* field in the output of the **show ethernet cfm domain** privileged EXEC command and the *Mep-Up* field in the output of the **show ethernet cfm maintenance-points remote crosscheck** privileged EXEC command might appear as *No* even if the CCM is learned in the remote database.

  This is expected behavior. The workaround is to use the **ethernet cfm mep crosscheck start-delay** command to set the delay-start timer value larger than the continuity-check interval. (CSCtf30542)‘

Configuration

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

- 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 dynamic ARP inspection is enabled on a switch, 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)

- 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)

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

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

EtherChannel

- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

  ```
  15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
  (ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
  4CEB50 859DF4 A7BF28 A98260 882658 879A58
  ```

  There is no workaround. (CSCsh12472)

IP

- 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)

IP Service Level Agreements (SLAs)

- When the IP SLAs configured reaction type (configured by entering the **ip sla reaction-configuration** global configuration command) is round-trip time (RTT), an RTT event causes duplicate SNMP traps.

  There is no workaround.

MAC Addressing

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

- The switch does not support tunnel interfaces, including DVMRP and PIM tunneling.
- 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 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)
- 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)

REP

- Although you can configure a REP segment without configuring REP edge ports, we recommend that you configure REP edge ports whenever possible because edge ports enable these functions:
  - selecting the preferred alternate port
  - configuring VLAN load balancing
  - configuring topology change notifications (TCNs) toward STP, other REP segments, or an interface
  - initiating the topology collection process
  - preemption mechanisms

  You cannot enable these functions on REP segments without edge ports.
- On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1000 milliseconds (1 second), the REP link flaps if the BFD interface is shut down and then brought back up.

  The workaround is to use the **rep lsl-age-out timer** interface configuration command to configure the REP LSL age timer for more than 1 second. (CSCsz40613)

Routing

- The switch does not support tunnel interfaces for routed traffic.
- 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)
- 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)

QoS

- 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 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. (CSCsb98219)

- When several per-port, per-VLAN parent policies are attached to the input of one or more interfaces and a child policy of these parent policies is modified, the parent policies are detached from the interfaces and reattached during the process. Because the modified policy is large, the TCAM entries are being used up, and the attached policies should be removed. However, some of the parent policies are not removed from the interface, and the TCAM entries are cleared. If you save the configuration and reload the switch, the policies are detached, but the TCAM is full, and you cannot attach other policies.

  This error message appears:

  ```
  QOSMGR-4-QOS_TCAM_RESOURCE_EXCEED_MAX: Exceeded a maximum of QoS TCAM resources
  ```

  The workaround is to manually detach the policy maps from all the interfaces by entering the **no service-policy input** *policy-map-name* interface configuration command on each interface. (CSCsk58435)

- When CPU protection is disabled, you can configure 64 policers per port on most switches. However, on Cisco ME 3400EG-12CS and Cisco ME 3400G-12CS switches, due to hardware limitations, you can attach 64 per-port, per-VLAN policers to a maximum of 6 ports. If you attempt to attach more than 6 per-port, per-VLAN 64-policer policy maps, the attachment fails.

  There is no workaround. (CSCsv21416)

SPAN and RSPAN

- The egress SPAN data rate might degrade when 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 multicast routing is disabled, egress SPAN is not degraded.

  There is no workaround. If possible, disable multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)

- 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)

- When system jumbo MTU size is configured on a switch and the egress ports can support jumbo frames, the egress SPAN jumbo frames are not forwarded to the SPAN destination ports.

  There is no workaround. (CSCsj21718)

- 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

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

VLAN

- If the number of VLANs times the number of trunk ports exceeds 13,000, the switch can stop.

  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)

Important Notes

- When you upgrade the switch software to Cisco IOS release 12.2(50)SE or higher and autonegotiation is enabled on a Gigabit SFP fiber switch port (the default), but disabled on the link partner port, the switch port interface can show a state of down/down while the link partner shows up/up. This is expected behavior.

  The workaround is to either enable autonegotiation on the link partner port or enter the **speed nonegotiate** interface command on the SFP port.

Open Caveats

- CSCtf77937 (Cisco ME 3400E only)

  When an EtherChannel is configured for 802.1ad and a channel member that is up is removed from the EtherChannel, the 802.1ad configuration is removed. However, if the port channel is shut down and then removed from the EtherChannel, the 802.1ad configuration is not removed.

The workaround is to enter the **no shutdown** interface configuration command on the port channel before removing it from the EtherChannel.

- CSCtf27594

  When Bidirectional Forwarding Detection (BFD) is enabled on an interface of a switch that is running Cisco IOS Release12.2(50)SE or later, Release 12.2(52)SE or later, or Release 12.2(54)SE, CPU spikes can occur once or twice per hour.

  There is no workaround.

- CSCtf71229 (Cisco ME 3400E only)

  On a Catalyst ME 3400E switch, the Gigabit Ethernet interface of an SFP module on which autonegotiation is disabled unexpectedly operates in half-duplex mode and then enters the suspended state when one of these conditions occur:

  – you restart a switch that is running Cisco IOS Release 12.2(50)SE3 or later, Release 12.2(53)SE or later, or Release 12.2(54)SE.

  – you reinsert the optical cable into the SFP module.

  – you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the EtherChannel interface to which the Gigabit Ethernet interface belongs.

  The workaround is to enter the **duplex auto** and **speed auto** interface configuration commands on the Gigabit Ethernet interface.

Resolved Caveats

- CSCsk00594

  Although visible in the command-line help, the **conform-action color** *class-map* police configuration command is not supported. Entering the command has no affect.

  There is no workaround.

- CSCsl14567

  When the status of a Resilient Ethernet Protocol (REP) primary edge port changes, for example, because you enter the **no shutdown** interface configuration command, the switch sends duplicate SNMP messages for the crepPortRoleChange trap.

  There is no workaround.

- CSCsx97605

  The CISCO-RTTMON-MIB is not correctly implemented.

- CSCsz18634

  On a switch running Cisco IOS release 12.2(46)SE, the output of the **show interfaces** privileged EXEC command shows 0 packets for port channel input and output rates.

  The workaround is to reload the switch by entering the **reload** privileged EXEC command.

- CSCtb10158

  A switch can fail when an SNMP process attempts to configure 802.1x authentication when it is already configured.

  There is no workaround.

- CSCtc43231

  A switch does not receive SNMP trap and inform messages from the correct interface after you enter the **snmp-server trap-source loopback0** and **snmp-server source-interface informs loopback0** global configuration commands.

  There is no workaround.

- CSCtc59162

  Modifying a prefix list that is configured as an inbound or outbound distribute-list causes the EIGRP peer to resynchronize.

  There is no workaround

- CSCtd29049

  A switch with at least one configured trunk port might fail when you use the **vlan** *vlan-id* global configuration command to configure more than 950 VLANs.

  There is no workaround.

- CSCte52821

  When you enter the **no ip ftp passive** global configuration command to allow all types of FTP connections on a switch running Cisco IOS Release 12.2(52)SE, FTP sessions could disable Telnet or console connections. You can no longer use the vty.

  The workaround is to restart the switch. To prevent FTP sessions from disabling Telnet or console connections, enter the **ip ftp passive** global configuration command.

- CSCte67201

  On a switch configured for IP routing and running Cisco IOS Release 12.2(50)SE or later, Cisco Express Forwarding (CEF) can use a large amount of memory. The IP RIB update process uses about 2000 bytes for each prefix that CEF uses.

  There is no workaround. You can reduce the memory use by reducing the number of routes that the switch processes.

- CSCte71904

  When you use the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command on a Resilient Ethernet Protocol (REP) primary edge port to block a VLAN list on one port and then use the same command to block another VLAN list on another port, the original port number and VLAN list are not overwritten. After you have blocked a VLAN list on one port, you cannot block another VLAN list on another port.

  There is no workaround.

- CSCte72365

  After upgrading from Cisco IOS Release 12.2(52)SE to Cisco IOS Release 12.2(53)SE, EIGRP hello packets are flooded on access ports of other subnets. This also occurs when you send pings to the broadcast address of other subnets.

  The workaround is to downgrade the image to Cisco IOS Release 12.2(52)SE.

- CSCtf89939

  When you have configured REP segment topology change notices (STCNs) and VLAN load balancing on an interface, entering the **shutdown** and the **no shutdown** command on the interface can cause a memory leak or can cause the switch to reload.

  There is no workaround.

Documentation Updates

Note For information about ME 3400 support for ingress QoS classification on QinQ-based ports, see the *Configuring ME 3400E QoS Classification for QinQ-Based Service, Release 12.2(53)SE* document under the ME 3400E Configuration Guides link.

Updates to the Software Configuration Guides - Cisco IOS Release 12.2(54)SE

"Configuring VLANs" Chapter

In the section *UNI-ENI VLANs*, the following statement was removed: "The switch supports a combination of only eight UNIs and ENIs in a UNI-ENI community VLAN."

The following statement was added: "There is no restriction to the number of UNIs and ENIs that you can add to a community VLAN or private VLAN."

"Configuring QoS" Chapter

In the section on *Aggregate Policing*, the statement referring to aggregate policers used to police traffic across VLANs is not correct. Aggregate policing across VLANs in per-port, per-vlan policy-map is not supported.

The example of aggregate policing used to regulate traffic across VLANs is not valid and will be removed.

"Configuring IP Unicast Routing" Chapter

In the section on *Configuring BFD, Disabling BFD Echo Mode:*

- The document states that you can enter the **no bfd echo** interface config command to disable echo mode and then configure the control-packet exchange rate by entering the **bfd slow-timer** global config command. This is incorrect. When BFD echo is disabled, the BFD slow-timer configuration does not apply. In a BFD session running in asynchronous mode, BFD packets are exchanged at a negotiated duration when the session is up and at the BFD slow-timer value when the session is down.
- The section states that disabling BFD echo on an interface disables only the sending of echo packets and the receiver of an echo packet always reflects it back to the sender. This is incorrect. In the Cisco IOS implementation of BFD, when BFD echo is disabled at one end of a link, the other end of the link also does not send echo packets and does not reflect back the echo packet.

ME 3400E "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling" Chapter - Update

When you configure selective QinQ to tunnel the traffic of two different customers on different S-VLANs, if the native VLAN (VLAN 1) is on one of the selective QinQ interfaces, untagged CDP and STP VLAN 1 packets are leaked to the other customer switches.

The workaround is to use the **switchport trunk native vlan** *vlan-id* interface configuration command to configure the native VLAN ID on an interface tunneling S-VLANs. For example, if you configured QinQ by entering the **switchport vlan mapping 1-100 dot1q-tunnel 500** command, you should also enter the **switchport trunk native vlan 500** command.

ME 3400E "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling" Chapter - New Section

Configuring IEEE 802.1ad

The Cisco ME 3400E switches support QinQ, a Cisco-proprietary system to enable double-tagging to provide VLAN scalability in the provider network, and Layer 2 protocol tunneling for tunneling customer control packets. IEEE 802.1ad uses standard protocols to solve VLAN scalability in provider networks. As with QinQ, data traffic entering from the customer interface is tagged with a service-provider tag. The customer frame crosses the provider network with two tags: the inner tag is the customer tag (C-tag). and the outer tag is the service-provider tag (S-tag). Control packets appear as data inside the provider network.

See this document for a description of IEEE 802.1ad support on Cisco provider bridges with commands:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_802_1ad.html

The Cisco ME 3400E switches support these features:

- a switchport-based model
- all-to-one bundling
- service multiplexing (complex UNI)

In IEEE 802.1ad, a switchport is configured as either a customer user-network interface (C-UNI), a service-provider UNI (S-UNI), or a network-to-network interface (NNI). Only Layer 2 interfaces can be 802.1ad ports.

- C-UNI—This port can be either an access port or an 802.1Q trunk port. The port uses the customer bridge addresses. To configure a C-UNI port, enter the **ethernet dot1ad uni c-port** interface configuration command. New keywords added to the **switchport vlan mapping** interface configuration command allow all-to-one or selective bundling capability for customer VLANs when the interface is configured as an 802.1ad trunk C-UNI port.
- S-UNI—This is an access port that provides the same service to all customer VLANs entering the interface, marking all C-VLANs entering the port with the same S-VLAN. In this mode, the customer's port is configured as a trunk port, and traffic entering the S-UNI is tagged. On S-UNIs, CDP and LLDP are disabled, and STP BPDU filtering and Port Fast are enabled. The port can be configured only as an access port; trunk configuration is not allowed.
  - CFM C-VLAN configuration is not allowed on an S-UNI.
  - On an ME 3400E switch, you enter the **ethernet dot1ad uni s-port** interface configuration command on an access port with an access VLAN.
- NNI—Entering the **ethernet dot1ad nni** interface command on a trunk port creates 802.1ad EtherType (0x88a8) and uses S-bridge addresses for CPU-generated Layer 2 protocol PDUs. Only trunk ports can be NNIs. CFM C-VLAN configuration is not allowed on an NNI.

See the "Updates to the ME 3400E Command Reference - Release 12.2(54)SE" section on page 30 for new commands or keywords added for this feature.

802.1ad Configuration Guidelines

- An S-UNI must be an access port.
- An NNI must be a trunk port.
- A C-UNI can be either an access port or a trunk port.
- On Cisco ME 3400 E switches, 802.1ad is a port-based feature. There is no global command for enabling 802.1ad. By default, without 802.1ad, all switchports are traditional 802.1Q ports.
- When 802.1ad is enabled, the tunneling of customer data frames is done in software. If the incoming BPDU rate is high, there could be some impact on CPU utilization.
- The switches do not support 802.1ad on EVCs or 802.1ad Layer 3 termination.
- The switches do not support split horizon on 802.1ad interfaces.
- You cannot enable Layer 2 protocol tunneling on 802.1ad interfaces. The features are mutually exclusive.
- ME 3400E switches support a mixed configuration model for 802.1ad that allows traditional Q-in-Q tunnels and 802.1ad tunnels on a bridge at the same time. When configuring a switch in mixed configuration mode, be sure to separate the broadcast domains for traditional 802.1Q tunneling and 802.1ad tunneling. To ensure functionality, do not configure 802.1ad NNI trunk ports and 802.1Q egress trunks with overlapping sets of allowed VLANs.
- By default, customer UDLD packets are tunneled on 802.1ad S-UNI ports and are processed (peered) on C-UNI ports. End-to-end UDLD is not supported on 802.1ad C-UNI ports.
- On ME 3400E switches, 802.1ad port types (C-UNI, S-UNI, NNI) are mutually exclusive with interface port types (NNI, UNI, ENI). You cannot change the port type configuration on an interface configured for 802.1ad.
- When configuring the service provider network for 802.1ad, be sure to configure 802.1ad NNIs on all interconnecting trunk ports. This is required for end-to-end functionality for customer Layer 2 PDUs in the service provider network.

Configuring 802.1ad on EtherChannels

When configuring 802.1ad on port channels, configure the EtherChannel group first, and then configure 802.1ad port configuration on the bundled port (port channel). When configured on the EtherChannel port channel, the 802.1ad configuration is applied to all ports in the port channel.

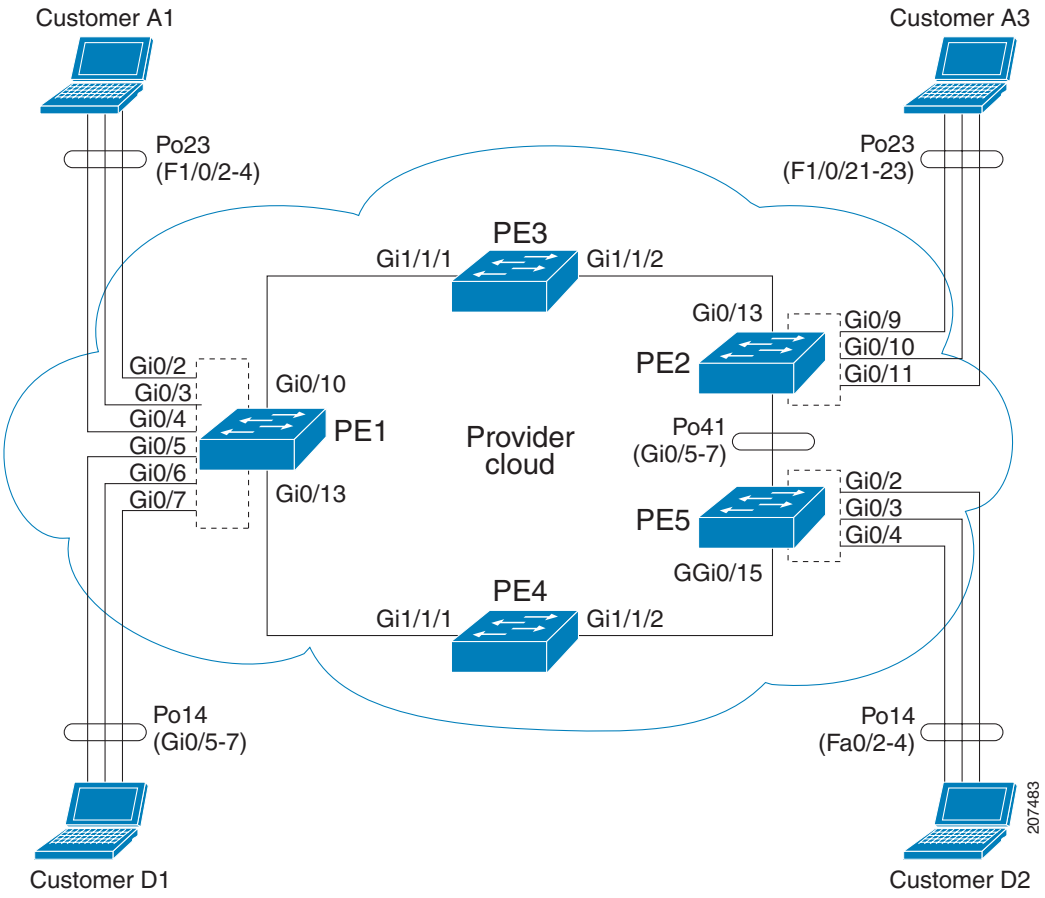
You cannot add a port to an EtherChannel if the port already has 802.1ad enabled.

Follow this configuration sequence when both CE and PE devices are actively participating in PAgP or LACP EtherChannels.

Configuration Example for 802.1ad End-to-End PAgP EtherChannels between CE Devices

For end-to-end PAgP EtherChannel tunneling between CE devices, you should extend the CE connections through the service provider network as a point-to-point service when the PE device has no EtherChannels in **on** mode. See the software configuration guide section "Configuring Layer 2 Tunneling for EtherChannels" in the "Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling" chapter. The same procedure applies to 802.1ad tunnels.

Figure 1 802.1ad End-to-End PAgP EtherChannels



Configuration on Customer A1:

```
Switch #show etherchannel summary
       Flags:  D - down        P - bundled in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
```

```
 R - Layer3      S - Layer2
 U - in use      f - failed to allocate aggregator

 M - not in use, minimum links not met
 u - unsuitable for bundling
 w - waiting to be aggregated
 d - default port
 Number of channel-groups in use: 2
 Number of aggregators:           2

Group  Port-channel  Protocol                          Ports
 ------+-------------+-----------+-----------------------------------------------
   23     Po23(SU)        PAgP (desirable)      Fa1/0/2(P)  Fa1/0/3(P)  Fa1/0/4(P)
```

Configuration on PE-1:

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk

Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# ethernet dot1ad uni s-port
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/10
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# media-type sfp
Switch (config-if)# ethernet dot1ad nni
```

Configuration on PE-3

```
Switch (config)# interface GigabitEthernet1/1/1
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk dot1q ethertype 88A8
Switch (config-if)# udld port aggressive
Switch (config-if)# ethernet dot1ad nni

Switch (config)# interface GigabitEthernet1/1/2
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk dot1q ethertype 88A8
Switch (config-if)# udld port aggressive
Switch (config-if)# ethernet dot1ad nni
```

Configuration on PE-2

```
Switch (config)# interface GigabitEthernet0/9
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/10
Switch (config-if)# switchport access vlan 4001
```

```
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/11
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# ethernet dot1ad uni s-port

Switch (config)# interface GigabitEthernet0/13
Switch (config-if)# switchport trunk allowed vlan 4001-4094
Switch (config-if)# switchport mode trunk
Switch (config-if)# ethernet dot1ad nni
```

Configuration on Customer A3

```
Switch (config)# interface Port-channel23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk

Switch (config)# interface FastEthernet1/0/21
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Switch (config)# interface FastEthernet1/0/22
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable

Switch (config-if)# interface FastEthernet1/0/23
Switch (config-if)# switchport trunk encapsulation dot1q
Switch (config-if)# switchport mode trunk
Switch (config-if)# channel-protocol pagp
Switch (config-if)# channel-group 23 mode desirable
```

Configuration with 802.1ad C-UNI port on PE-2 and PE-3

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4002
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/3
Switch (config-if)# switchport access vlan 4001
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4001
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4001
Switch (config-if)# Ethernet dot1ad uni c-port

Switch (config)# interface GigabitEthernet0/4
Switch (config-if)# switchport access vlan 4003
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4003
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4003
Switch (config-if)# Ethernet dot1ad uni c-port
```

The configuration on other switches remains the same in the 802.1ad C-UNI scenario.

New Section for the "Configuring Ethernet OAM, CFM, and E-LMI" Chapter

Configuring CFM on C-VLAN (Inner VLAN)

The previous implementation of IEEE 802.1ag CFM allows provisioning of maintenance points on the S-VLAN component. It does not allow monitoring or troubleshooting when QinQ is enabled on the provider-edge (PE) device. This release allows customers to provision maintenance intermediate points (MIPs) and Up maintenance endpoints (MEPs) on the C-VLAN (inner VLAN) component of QinQ or 802.1ad ports to provide visibility on the C-VLAN. In addition, some C-VLAN restrictions are removed and C-VLANs are now supported on 802.1q tunnel ports.

For more information about this feature and the supported commands, see:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_cvlan.html

This section describes the functionality supported on the Cisco ME 3400E and ME 3400 switches.

Platform Support

- 802.1q-tunnel-port mode: Cisco ME 3400E and ME 3400 switches.
- Selective Q-in-Q (support for 1-to-2 VLAN mapping, but not 1-to-1 VLAN mapping): ME 3400E switches only.
- 802.1ad UNI (only C-UNI 1-to-2 mapping): ME 3400E switches only.

Feature Support and Behavior

CFM S-VLAN component support:

- Up MEPs at any level (0 to 7).

  Up MEPs use the port access VLAN ID (the outer tag or S-VLAN).

  CFM frames sent and received by Up MEPs have a single VLAN tag, and the VLAN identifier is the port access VLAN ID (S-VLAN). Because the 802.1q tunnel interface marks the endpoint of the S-VLAN, the associated S-VLAN component should mark the endpoint of the CFM domain running over the S-VLAN space.

CFM C-VLAN component support:

- Up MEP functions at any level (0 to 7).

  Up MEPs use two tags: an outer tag with a VLAN ID that is the port access VLAN (S-VLAN) and an inner tag with a selected C-VLAN that is allowed through the 802.1q tunnel port. CFM frames sent and received by these Up MEPs are always double-tagged.
- MIP functions at any level (0 to 7).

  MIPs process CFM frames that are single-tagged when coming from the wire-side and double-tagged when coming from the relay-function side.
- Transparent point functions.

Port MEP frames are always sent untagged, even when the **dot1q vlan native** tag is enabled.

Supported maintenance points on 802.1q tunnels:

- Up MEP on the C-VLAN component for selective or all-to-one bundling
- Up MEP on the S-VLAN
- Port MEP
- MIP support on C-VLAN component for selective or all-to-one bundling

Note The switch supports only manual configuration of MIPs. It does not support MIP autocreation on C-VLANs.

Platform Restrictions and Limitations

- Maximum supported MEPs per switch at each continuity check message (CCM) interval:
  - 1600 MEP local and 1600 MEP remote (on C-VLAN and S-VLAN) with 10-second intervals
  - 250 MEP local and 250 MEP remote (on C-VLAN and S-VLAN) with 1-second intervals
  - 30 MEP local and 30 MEP remote (on C-VLAN and S-VLAN) with 100-ms intervals
- Maximum supported MIPs at each CCM interval:
  - 300 MIPs at 10 seconds
  - 125 MIPs at 1 second
  - 30 MIPs at 100 ms
- There could be issues detecting cross-connect errors on ME 3400 switches.
- These features are not supported:
  - CFM C-component on the native VLAN
  - Port-based and VLAN-based MPLS (pseudowire) on the C-VLAN
  - Down MEP on S or C-VLAN (provider network port)
  - MIP on S-VLAN (provider network port)
  - CFM C-VLAN alarm indication signal (AIS)
  - CFM C-VLAN locked signal (LCK)
  - 802.3ah interworking with CFM C-VLAN
  - CFM C-VLAN IP SLAs
  - CFM C-VLAN E-LMI
  - CFM C-VLAN MIP autocreation.

“Supported MIBs” Appendix

The IEEE-compliant CFM MIB (IEEE CFM MIB) provides MIB support for IEEE 802.1ag compliant CFM (IEEE CFM) services. The IEEE CFM MIB can be used as a tool to trace paths, verify and manage connectivity, and detect faults in a network.

For information about the IEEE CFM MIB and the services it supports, see this URL:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_mib.html

"Unsupported Commands" Appendix

These IP unicast routing commands are now supported:

set tag (route-map configuration)

ip prefix-list (global configuration)

ip as-path access-list (global configuration)

These CGMP commands are *not* supported:

ip cgmp (interface configuration)

clear ip cgmp (privileged EXEC)

Updates to the Software Configuration Guides - Cisco IOS Release 12.2(53)SE

"Configuring QoS" Chapter: New Supported Features

Ingress class-default Support in Per-Port, Per-VLAN Policies (ME 3400 and 3400E)

In past releases in a per-port, per-VLAN hierarchical input policy-map, you could not associate a child policy with the class **class-default** of the parent policy map. You could only classify on known VLANs received on a port. In Cisco IOS Release 12.2(53)SE, you can now enter **class class-default** in the parent policy map of a per-port, per-VLAN hierarchical input policy map to classify all VLANs not identified by specified parent VLAN classes. You can then associate a child-policy to this parent *class class-default* by using the **service-policy** *child-policy-map name* policy-map class configuration command to specify child classes and actions to apply to this traffic.

In this sample configuration, the child policy map *child-policy-1* is associated with the class *customer1-vlan* and *child policy-2* is associated with all other traffic.

```
Switch(config)# policy-map uni-parent
Switch(config-pmap)# class customer1-vlan
Switch(config-pmap-c)# service-policy child-policy-1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# service-policy child-policy-2
Switch(config-pmap-c)# exit
```

These same limitations from past releases about combinations of child-policies with a particular VLAN-ID in per-port, per-VLAN policies across the switch also apply to the **class-default** in per-port, per-VLAN policies.

- You cannot combine Layer 2 child policies classifying on S-COS, C-COS, or Layer 2 (MAC) ACLs *and* Layer 3 child policies classifying on DSCP, IP precedence or Layer 3 (IP) ACLs.
- You cannot combine a class default only child policy *and* a Layer 3 child policy classifying on DSCP, IP precedence, or Layer 3 (IP) ACLs.

Simultaneous Multifield and COS, IP DSCP, and IP Precedence QoS Classification (ME 3400 and 3400E)

In past releases, multifield classification using Layer-3 IP ACLs and DSCP classification simultaneously for every packet was not fully supported. You could configure either Layer-3 IP ACL classification or DSCP classification for every packet. Also multifield classification using Layer-2 MAC ACLs and COS classification simultaneously for every packet was not fully supported. You could configure either Layer-2 MAC-ACL classification or COS classification for every packet.

In Cisco IOS Release 12.2(53)SE, you can simultaneously configure multifield classification with Layer-3 IP ACLs and DSCP classification for every packet by using the IP access group to identify the required DSCP value to be classified along with other IP-header fields. You can also simultaneously configure multifield classification with Layer-2 MAC ACLs and COS classification for every packet by using the MAC access group to identify the COS value to be classified along with other MAC-header fields.

Ingress QoS Classification Scalability Enhancements (ME 3400 and 3400E)

In previous releases, ME 3400 and ME 3400E 24TS and 2CS models supported ingress QoS classification for 254 unique VLAN IDs on the switch. In Cisco IOS Release 12.2(53)SE, you can configure ingress QoS classification for 256 or more VLAN IDs (255 unique VLAN IDs plus the **class-default**, which can classify on all remaining VLAN-IDs).

In previous releases, ME 3400 and ME 3400E 12CS models supported ingress QoS classification for 254 unique VLAN IDs. In Cisco IOS Release 12.2(53)SE, you can configure ingress QoS classification for 1024 or more VLAN-IDs on the switch (255 unique VLAN IDs plus **class default**, which can classify on all the rest of the VLAN-IDs, on each set of four ports).

In Cisco IOS Release 12.2(53)SE, on ME 3400E switches, you can also classify on the inner VLAN-ID of QinQ packets on QinQ ports. There is no limit on any switch models to the number of inner VLAN IDs that can be classified in ingress QoS policies.

Updates to the Software Configuration Guides - Cisco IOS Release 12.2(52)SE

"Configuring Ethernet OAM, CFM, and E-LMI" Chapter

This information was added:

The Service Diagnostics 2.0 C FM diagnostic scripts is part of the 12.2(52)SE release. The script is available for download at:

http://www.cisco.com/en/US/prod/iosswrel/ps6537/ps6555/ps9424/cisco_ios_service_diagnostics_scripts.html

Refer to the Service Diagnostic 2.0 user guide at:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps9424/whitepaper_c11-566741.html

This information was corrected:

In the "Configuring the CFM Domain" section, Step 2 was to enter the **ethernet cfm ieee** global configuration command to configure the CFM version as IEEE 802.1ag.

This step is not required. If you are running Cisco IOS Release 12.2(52)SE, the CFM version is always 802.1ag, and the command is automatically generated when you enable CFM.

"Configuring IP Unicast Routing" Chapter

User Interface for VRF-Aware RADIUS

To configure VRF-Aware RADIUS, you must first enable AAA on a RADIUS server. This release supports the **ip vrf forwarding** *vrf-name* server-group configuration and the **ip radius source-interface** global configuration commands, as described in the *Per VRF AAA Feature Guide* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftvrfaaa.html

New Section for the "Configuring IEEE 802.1x Port-Based Authentication" Chapter

Common Session ID

Authentication manager uses a single session ID (referred to as a common session ID) for a client no matter which authentication method is used. This ID is used for all reporting purposes, such as the show commands and MIBs. The session ID appears with all per-session syslog messages.

The session ID includes:

- The IP address of the Network Access Device (NAD)
- A monotonically increasing unique 32 bit integer
- The session start time stamp (a 32 bit integer)

This example shows how the session ID appears in the output of the **show authentication** command. The session ID in this example is 160000050000000B288508E5:

```
Switch# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  160000050000000B288508E5
```

This is an example of how the session ID appears in the syslog output. The session ID in this example is also160000050000000B288508E5:

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

The session ID is used by the NAD, the AAA server, and other report-analyzing applications to identify the client. The ID appears automatically. No configuration is required.

Update to the "Configuring MSTP" Chapter

This guideline was added to the "MSTP Configuration Guidelines" section of the "Configuring MSTP" chapter:

- When the switch is in MST mode, it uses the long path-cost calculation method (32 bits) to compute the path cost values. With the long path-cost calculation method, these path cost values are supported:

Speed	Path Cost Value
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200

Updates to the ME 3400E Command Reference - Release 12.2(54)SE

These platform-specific commands were added or changed for this release:

- **switchport vlan mapping**
- **debug platform dot1ad**
- **rep block port**
- **show inventory**

switchport vlan mapping

To configure VLAN mapping on a trunk port, use the **switchport vlan mapping** interface configuration command with the **dot1q tunnel** keywords. You can configure one-to-one VLAN mapping, 802.1Q tunneling (QinQ) mapping, or selective QinQ mapping. To configure all-to-one or selective VLAN mapping on an 802.1ad C-UNI trunk port, use the command with the **dot1ad-bundle** keyword. To disable the configuration, use the **no** form of the command.

switchport vlan mapping *vlan-id* {*translated-id* | **dot1ad-bundle** *outer vlan id* | **dot1q tunnel** *translated-id*}

no switchport vlan mapping *vlan-id* {*translated-id* | **dot1ad-bundle** *outer vlan id* | **dot1q tunnel** *translated-id*}

switchport vlan mapping default {**dot1ad-bundle** *outer vlan id* | **dot1q tunnel** *translated-id* | **drop**}}

no switchport vlan mapping default {**dot1ad-bundle** *outer vlan id* | **dot1q tunnel** *translated-id* | **drop**}}

no switchport vlan mapping all

Syntax Description

vlan-id	Specifies the original (customer) VLAN or VLANs (C-VLANs), also known as the VLAN on the wire, for one-to-one or selective QinQ mapping. You can enter multiple VLAN IDs separated by a comma or a series of VLAN IDs separated by a hyphen (for example 1,2,3-5). The range is from 1 to 4094.
translated-id	Specifies the translated VLAN-ID: the S-VLAN to be used in the service provider network. The range is from 1 to 4094.
default	Specify the default for C-VLANs other than those specified.
dot1ad-bundle *outer vlan-id*	Specifies 802.1ad bundling on an 802.1ad C-UNI trunk port. • Enter after the **default** keyword to select all-to-one bundling. • Enter after *vlan-id* to select selective bundling. The outer VLAN ID range is from 1 to 4094. **Note** This command is available only on 802.1ad trunk C-UNI ports.
dot1q-tunnel *translated-id*	Adds a translated VLAN-ID to specify a VLAN tunnel (add an outer S-VLAN tag) on a trunk port. The range of the S-VLAN tag is 1 to 4094. Use these keywords for traditional QinQ mapping.

drop	Specify that VLANs other than the C-VLAN or VLANs specified are dropped. Use this keyword for one-to-one or selective QinQ mapping.
all	In the **no switchport vlan mapping** command, specifies that all VLAN mapping configurations on the interface are deleted.

Defaults

No VLAN mapping is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(44)EY	This command was introduced.
12.2(54)SE	The **dot1ad-bundle** *outer vlan id* keywords were added.

Usage Guidelines

Before configuring VLAN mapping on an interface, enter the **switchport mode trunk** interface configuration command to configure the interface as a trunk port.

You configure VLAN mapping on ports connected to the customer network. which are typically user network interfaces (UNIs). However, you can also configure VLAN mapping on an network node interfaces (NNIs) or on enhanced network interfaces (ENIs).

For 802.1ad, VLAN mapping is permitted only on 802.1ad C-UNI trunk ports. VLAN mapping is not supported on S-UNI and NNI interfaces.

You can configure VLAN mapping on a physical interface or on a port channel of multiple interfaces that have the same configuration.

For 802.1Q VLAN mapping:

- To configure one-to-one VLAN mapping, use the **switchport vlan mapping** *vlan-id translated-id* command.
- To configure traditional QinQ (VLAN bundling) on an interface, enter the **switchport vlan mapping default dot1q-tunnel** *outer vlan-id.* This is the same as configuring the interface as a tunnel port and mapping all VLANs to the specified S-VLAN ID.

Note To avoid mixing customer traffic, when you configure traditional QinQ on a trunk port, you should use the **switchport trunk allowed vlan** *vlan-id* interface configuration command to configure the outer VLAN ID (S-VLAN) as an allowed VLAN on the trunk port.

- To configure selective QinQ on an interface, enter the **switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id* command.

  You can configure one-to-one mapping and selective QinQ on the same interface, but you cannot use the same C-VLAN IDs in both configurations.

For one-to-one mapping and selective QinQ, or for default all-to-one 802.1ad VLAN mapping, you can use the **default drop** keywords to specify that traffic is dropped unless the specified C-VLAN ID and S-VLAN ID combination is explicitly translated.

The **no** form of the **switchport vlan mapping** commands clears the specified mapping configuration on the interface. The **no switchport vlan mapping all** command clears all mapping configurations on the interface.

On an ME-3400E interface configured for VLAN mapping, mapping to the S-VLAN occurs on traffic entering the switch. Therefore, when you configure other features on an interface configured for VLAN mapping and a VLAN ID is required, use the S-VLAN ID. The exception is when configuring VLAN mapping and Ethernet E-LMI on an interface. Use the C-VLAN in the **ethernet lmi ce-vlan map** *vlan-id* service-instance configuration mode command.

You cannot configure **encapsulation replicate** on a SPAN destination port if the source port is configured as a tunnel port or has a one-to-two mapping configured. Encapsulation replicate is supported with one-to-one VLAN mapping.

For VLAN mapping on 802.1ad C-UNI trunk ports:

- You use the **dot1ad-bundle** keywords to achieve all-to-one and selective bundling functionality on a C-UNI trunk port. The default mapping is one-to-one on the source VLAN.
- You can configure 802.1ad only on C-UNI trunk ports. This command is not supported on S-UNIs or NNIs.

Examples

This example shows how to use one-to-one mapping to map VLAN IDs 1 and 2 in the customer network to VLANs 1001 and 1002 in the service-provider network and to drop traffic from other VLAN IDs.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport vlan mapping 1 1001
Switch(config-if)# switchport vlan mapping 2 1002
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

This example shows how to use traditional QinQ to bundle all traffic on the port to leave the switch with an S-VLAN ID of 10.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport vlan mapping default dot1q-tunnel 10
Switch(config-if)# exit
```

This example shows how to configure selective QinQ mapping on the port so that traffic with a C-VLAN ID of 5, 7, or 8 would enter the switch with an S-VLAN ID of 100. The traffic of any other VLAN IDs is dropped.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport vlan mapping 5, 7-8 dot1q-tunnel 100
Switch(config-if)# switchport vlan mapping default drop
Switch(config-if)# exit
```

This example shows how to configure default all-to-one 802.1ad VLAN mapping on a C-UNI port:

```
Switch (config)# interface GigabitEthernet0/2
Switch (config-if)# switchport access vlan 4002
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan 4002
Switch (config-if)# switchport vlan mapping default dot1ad-bundle 4002
Switch (config-if)# Ethernet dot1ad uni c-port
Switch(config-if)# exit
```

This example shows how to configure selective 802.1ad VLAN mapping on the port.

```
Switch(config)# interface gigabitethernet0/1
Switch (config-if)# switchport mode trunk
Switch(config-if)# switchport vlan mapping 5, 7-8 dot1ad-bundle 100
```

```
Switch(config-if)# switchport vlan mapping default drop
Switch (config-if)# Ethernet dot1ad uni c-port
Switch(config-if)# exit
```

Related Commands

Command	Description
show vlan mapping	Displays VLAN mapping information.

debug platform dot1ad

To enable debugging of IEEE 802.1ad tagging, use the **debug platform dot1ad** privileged EXEC command. To disable debugging, use the **no** form of the command.

debug platform dot1ad [**error** | **events** | **receive** | **transmit**]

no debug platform dot1ad [**error** | **events** | **receive** | **transmit**]

Syntax Description

error	Displays 802.1ad error messages.
events	Displays 802.1ad event debug messages.
receive	Displays 802.1ad receive debug messages.
transmit	Displays 802.1ad sent debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(54)SE	This command was introduced.

Usage Guidelines

The **undebug platform dot1ad** command is the same as the **no debug platform dot1ad** command.

When you enter **debug platform dot1ad** with no keywords, all 802.1ad debug messages appear.

Related Commands

Command	Description
show debugging	Displays information about the enabled types of debugging.

rep block port

These usage guidelines were added:

- There is no limit to the number of times that you can enter the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command. You can block an unlimited number, range, or sequence of VLANs.
- When you use the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command on a Resilient Ethernet Protocol (REP) primary edge port to block a VLAN list and then use the same command to block another VLAN list on the same port, the second VLAN list does not replace the first VLAN list but is appended to the first VLAN list.
- When you use the **rep block port id** *port-id* **vlan** *vlan-list* interface configuration command on a REP primary edge port to block a VLAN list on one port and then use the same command to block another VLAN list on another port, the original port number and VLAN list are overwritten.

show inventory

This usage guideline was added:

- For the product identifier (PID) and version identifier (VID) of SFP modules, the output of the **show inventory** user EXEC command displays either the correct information or displays *Unspecified* for the PID and nothing for the VID if the SFP module does not have PID and VID information.

Update to the ME 3400 Hardware Installation Guide

Cisco Ethernet Switches are equipped with cooling mechanisms, such as fans and blowers. However, these fans and blowers can draw dust and other particles, causing contaminant buildup inside the chassis, which can result in a system malfunction.

You must install this equipment in an environment as free as possible from dust and foreign conductive material (such as metal flakes from construction activities).

Follow these standard for guidelines for acceptable working environments and acceptable levels of suspended particulate matter:

- Network Equipment Building Systems (NEBS) GR-63-CORE
- National Electrical Manufacturers Association (NEMA) Type 1
- International Electrotechnical Commission (IEC) IP-20

Updates to the System Message Guide

These messages were added to the system message guide:

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action. AuditSessionID [chars]`

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication. [chars] is the session ID.

Recommended Action Reduce other system activity to reduce memory demands.

Error Message `DOT1X-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation The authentication was unsuccessful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `%DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Recommended Action The authentication result was overridden. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Explanation No action is required.

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation Authentication was successful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars] AuditSessionID [chars]`

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. This message might appear if IEEE 802.1x is enabled. [enet] is the client MAC address, the first [chars] is the interface, and the second [chars] is the session ID.

Recommended Action If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, remove it from that port.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_PRIMARY_VLAN: Attempt to assign primary VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a primary VLAN to an IEEE 802.1x port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Use a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a nonsecondary VLAN to a private VLAN host IEEE 802.1x port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the mode of the port so that it is no longer a PVLAN host port or use a valid secondary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure the primary VLAN exists and is not shut down. Verify that the private VLAN is associated with a primary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host port, which is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the mode of the port so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN.

Error Message `DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port that is configured as a Switched Port Analyzer (SPAN) destination port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the SPAN configuration so that the port is no longer a SPAN destination port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN AuditSessionID [chars]`

Explanation An attempt was made to assign a data VLAN to an IEEE 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change either the voice VLAN or the IEEE 802.1x-assigned VLAN on the interface so that they are not the same.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is used internally and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Explanation Assign a different VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign an invalid VLAN to an IEEE 802.1x port. The VLAN specified is out of range. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Update the configuration to use a valid VLAN.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [chars] to 802.1x port [chars] AuditSessionID [chars]`

Explanation An attempt was made to assign a VLAN to an IEEE 802.1x port, but the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Make sure the VLAN exists and is not shutdown or use another VLAN.

These messages were deleted but are still in the system message guide:

Error Message `DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action.nn`

Error Message `DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars]`

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars]`

Error Message DOT1X_SWITCH-5-ERR_INVALID_PRIMARY_VLAN: Attempt to assign primary VLAN [dec] to 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination

Error Message DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN.

Error Message DOT1X_SWITCH-5-ERR_VLAN_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_VLAN_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [dec] to 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_VLAN_ON_ROUTED_PORT: Dot1x cannot assign a VLAN [dec] to a routed port [chars]

Error Message DOT1X_SWITCH-5-ERR_VLAN_PROMISC_PORT: Attempt to assign VLAN [dec] to promiscuous 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_VLAN_RESERVED: Attempt to assign reserved VLAN [dec] to 802.1x port [chars]

Error Message DOT1X_SWITCH-5-ERR_VLAN_RSPAN: Attempt to assign RSPAN VLAN [dec] to 802.1x port [chars]. 802.1x is incompatible with RSPAN

Error Message SW_VLAN-4-VTP_USER_NOTIFICATION: VTP protocol user notification: [chars].

Updates to the ME 3400E Regulatory Compliance and Safety Information Guide and the Getting Started Guide

These warnings were incorrectly documented in the guides. These are the correct warnings:

All Switches

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than:**
10 A Statement 1005

Cisco ME 3400EG-2CS-A

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of:**
140°F (60°C) Statement 1047

Cisco ME 3400E-24TS-M and Cisco ME 3400EG-12CS-M

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of:**
149°F (65°C) Statement 1047

Related Documentation

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

- Cisco ME 3400E switch:

  http://www.cisco.com/en/US/products/ps9637/tsd_products_support_series_home.html
- Cisco ME 3400 switch:

  http://www.cisco.com/en/US/products/ps6580/tsd_products_support_series_home.html

These are combined documents for the switches:

- *Cisco ME 3400E, ME 3400, and ME 2400 Ethernet Access Switches System Message Guide*

These documents are available for the Cisco ME 3400E switch:

- *Release Notes for the Cisco ME 3400E Ethernet Access Switch*
- *Cisco ME 3400E Ethernet Access Switch Software Configuration Guide*
- *Cisco ME 3400E Ethernet Access Switch Command Reference*
- *Cisco ME 3400E Ethernet Access Switch Hardware Installation Guide*
- *Cisco ME 3400E Ethernet Access Switch Getting Started Guide*

- *Regulatory Compliance and Safety Information for the Cisco ME 3400E Ethernet Access Switch*

These documents are available for the Cisco ME 3400 switch:

- *Cisco ME 3400 Ethernet Access Switch Software Configuration Guide*
- *Cisco ME 3400 Ethernet Access Switch Command Reference*
- *Cisco ME 3400 and ME 2400 Ethernet Access Switch System Message Guide*
- *Cisco ME 3400 Ethernet Access Switch Hardware Installation Guide*
- *Cisco ME 3400 and ME 2400 Ethernet Access Switches Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco ME 3400 and ME 2400 Ethernet Access Switches*
- *Configuration Notes for the Cisco ME 3400G-12CS Ethernet Access Switch*

Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

SFP compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

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

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