Release Notes for the Cisco ME 3400E and ME 3400 Ethernet Access Switches, Cisco IOS Release 12.2(58)SE1 and Later

Revised: January 22, 2014

Note Cisco IOS Release 12.2(58)SE images for all platforms were removed from Cisco.com because of a severe defect, CSCto62631. The solution for the defect is in Cisco IOS Release 12.2(58)SE1.

Cisco IOS Release 12.2(58)SE1 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(58)SE1 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 26.

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

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

Contents

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

© 2011 Cisco Systems, Inc. All rights reserved.

Hardware Supported

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

Table 1 Supported Hardware (continued)

Device	Description	Supported by Minimum Cisco IOS Release
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		
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
Note	DOM status that helps monitor optical transceivers in the system generates system log every 600 seconds (10 minutes). This update period is not configurable. Reporting of changes in the status may lag behind the actual status changes due to the update rate.	
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

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.122-58.SE1.tar	Cisco ME 3400 metro base cryptographic image with Kerberos, Secure Shell (SSH), and basic Metro Ethernet features.
me340x-metroaccessk9-tar.122-58.SE1.tar	Cisco ME 3400E and ME 3400 metro access cryptographic image with Kerberos, SSH, and Layer 2 + Metro Ethernet features.
me340x-metroipaccess9-tar.122-58.SE1.tar	Cisco ME 3400E and ME 3400 metro IP access cryptographic image with 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/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

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

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/docs/ios/fundamentals/command/reference/cf_t1.html

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.

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:

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

http://www.cisco.com/cisco/software/navigator.html?a=a&i=rpm

b. Navigate to **Switches > Service Provider Switches - Ethernet Access**.

c. Navigate to your switch model.

d. Click **IOS Software**, then select the latest IOS release.

Download the image you identified in Step 1.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, 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 Software Features

- VACL Logging to generate syslog messages for ACL denied IP packets
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.
- IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates to support the IP version 6 (IPv6)-only and the IPv6 part of the protocol-version independent (PVI) objects and tables.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- Support for the Virtual Router Redundancy Protocol (VRRP) for IPv4, which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.
- Support for IPv4 and IPv6 Gateway Load Balancing Protocol (GLBP) for automatic router backup for IP hosts configured with a single default gateway on a LAN.
- Support for IPv6 DHCP server, client and relay in a virtual routing and forwarding (VRF) environment with limited VRF flexibility.

- Support for IPv6 Multi-Protocol VRF-CE (also referred to as VRF-Lite).
- Support for Layer 2 protocol tunneling for Link Layer Discovery Protocol (LLDP) traffic.

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
VACL logging	12.2(58)SE1
Call Home support	12.2(58)SE1
IP/IF MIBs for IPv6	12.2(58)SE1
NTPv4 over IPv6	12.2(58)SE1
DHCPv6 bulk lease query and DHCPv6 relay source configuration	12.2(58)SE1
RADIUS, TACACS+, and SSH/SCP over IPv6	12.2(58)SE1
VRRP version 4 support	12.2(58)SE1
GLBP for IPv4 and IPv6 with VRF-Lite	12.2(58)SE1
IPv6 unicast routing in VRF-Lite	12.2(58)SE1
VRF-aware IPv6 DHCP server and client support	12.2(58)SE1
802.1Q LLDP tunneling	12.2(58)SE1
Configuration of an alternate MTU value for specific interfaces	12.2(55)SE
BFD Protocol on SVIs	12.2(55)SE
Support for 802.1ad split horizon (ME 3400E).	12.2(55)SE
QoS classification and marking DEI bit in an IEEE 802.1ad frame (ME 3400E)	12.2(55)SE
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	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.	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

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

Feature	Minimum Cisco IOS Release Required
Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3).	12.2(52)SE
Support for including a hostname in the option 12 field of DHCPDISCOVER packets.	12.2(52)SE
DHCP snooping circuit-id sub-option of the Option 82 DHCP field.	12.2(52)SE
Connectivity fault management (CFM) Draft 8.1 compliance.	12.2(52)SE
Support for the TWAMP standard for measuring round-trip network performance between two devices.	12.2(52)SE
Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, HTTP, and 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.	12.2(52)SE
Resilient Ethernet Protocol (REP) hello link status layer (LSL) age timer configurable from 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
Support for the *, *ip-address*, **interface** *interface-id,* and **vlan** *vlan-id* keywords with the **clear ip dhcp snooping** command	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
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
Secure Copy Protocol	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
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)

- When an ME 3400 port is connected to an ME 3400E port, if one port is configured to 10 Mb/s and the other port is configured to 100 Mb/s (either full or half duplex), the 10 Mb/s port state appears as up/up and the 100 Mb/s port appears as down/down. This connection is a misconfiguration because the speed and duplex do not match.

  The workaround is to correct the misconfiguration. (CSCtg53462)

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)

- 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. CSCtf77937 (Cisco ME 3400E only)

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)
- If you configure two or more connected REP segments to send segment topology change notices (STCNs) by entering the **rep stcn segment** *segment-id* interface configuration command on REP interfaces, when segments inject messages simultaneously, an STCN loop occurs, and CPU usage can increase to 99 percent for 1 to 2 minutes before recovering.

  The workaround is to avoid configuring multiple STCNs in connected segments. This is a misconfiguration. (CSCth18662)

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)

- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

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

- CSCta39338

  When you globally enable UDLD by entering the **udld** {**aggressive | enable | message time** *message-timer-interval*} global configuration command, UDLD is now enabled only on fiber optic ports and on dual-purpose ports operating as fiber optic interfaces. It is not enabled on copper ports or dual-purpose ports operating as copper interfaces. For the **udld** global configuration command to enable UDLD on dual-purpose ports that have a small form-factor pluggable (SFP) module connected, you must explicitly configure the interface media type as SFP by entering the **media-type sfp** interface configuration command.

- CSCtg98453

  When you make port security changes on an interface, such as configuring aging time, violations, or aging type, error messages and tracebacks might appear.

  There is no workaround.

- CSCth33165 (ME 3400E only)

  – If you change the 802.1ad port type on an EtherChannel interface from s-uni isolate to c-uni (isolate or nonisolate), VLAN translation and EtherChannel incompatibility messages appear on the console. These messages do not appear for other port-type modifications.

There is no functionality impact. The messages appear because of timing-related issues when an 802.1ad port type is changed from s-uni isolate to c-uni (isolate or nonisolate). To avoid these messages, remove the s-uni isolate configuration by entering the **no ethernet dot1ad uni s-port isolate** command on the EtherChannel interface before entering the **ethernet dot1ad uni c-port** [**isolate**] command.

– When a new member port is dynamically added to an EtherChannel that is configured as an 802.1ad c-uni port (isolated or nonisolated) with VLAN mapping applied, no channel incompatibility message is seen, and the port is bundled into the EtherChannel. VLAN mapping is not applied to the new member port. If a new member port without the same VLAN mapping configuration is added to the channel interface, a VLAN mapping mismatch between the new port and the first active member of the port should be detected and an incompatibility error message should appear. Since VLAN mapping configuration is explicitly done by the user on an 802.1ad c-uni channel interface, the new port should not get bundled and should go into a suspended state.

The workaround is that before adding a port to an 802.1ad c-uni channel interface, you should explicitly configure the port with the same VLAN mapping as the EtherChannel to maintain configuration consistency.

- CSCth77918 (ME 3400E only)

  When the EtherChannel group mode is **on** and you configure 802.1ad split horizon on the EtherChannel interface by entering the **ethernet dot1ad uni s-port isolate** interface configuration command, after a switch reload, a PAgP flap error occurs, and the EtherChannel goes down. The problem is not seen with other 802.1ad port types or other EtherChannel modes (PAgP mode **desirable** or LACP mode **active** or **passive**).

  The workaround is to enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the error-disabled member ports of the EtherChannel. This removes the problem, and the Etherchannel comes up properly.

- CSCtj83964

  On a switch running Protocol-Independent Multicast (PIM) and Source Specific Multicast (SSM), multicast traffic might not be sent to the correct port after the switch reloads.

  The workaround is to enter the **clear ip route** privileged EXEC command or reconfigure PIM and SSM after a reload.

- CSCtl32991

  Unicast EIGRP packets destined for the switch are sent to the host queue instead of to the higher priority routing protocol queue.

Note This does not occur when packets are routed through the switch to another destination.

  There is no workaround.

- CSCtl60247

  When a switch running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

  There is no workaround.

- CSCtl51859

  Neighbor discovery fails for IPv6 hosts connected to the switch when the IPv6 MLD snooping feature is enabled globally on the switch.

  The workaround is to disable IPv6 MLD snooping on the switch.

- CSCtl81217

  When a switch is using a DHCP server to assign IP addresses and an interface on the switch has RIP enabled, if the switch reloads, the interface loses some RIP configuration (specifically RIP authentication mode and RIP authentication key-chain). This does not happen when the IP address is statically configured on the interface. The problem occurs only when you configure RIP before an IP address is assigned by the DHCP server.

  There is no workaround, but you can use an embedded event manager (EEM) script to add the interface configuration commands on the interface:

  ip rip authentication mode

  ip rip key-chain

Resolved Caveats

Caveats Resolved in Cisco IOS Release 12.2(58)SE2

- CSCtn91366 (Catalyst Switch ME-3400E)

  When the tunnel interface is configured with an ingress policy, the SP-VLAN and CE-VLAN tags are marked with CoS values on the egress SPAN packets. The SP-VLAN tag shows the correct CoS value that is marked, but the CE-VLAN shows the incorrect CoS value. Typically, the CE-VLAN must not be marked with a CoS value. This problem occurs when Selective QinQ is configured on the switch with the input policy set to re-mark CoS.

  There is no workaround.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCtq01926

  When you configure a port to be in a dynamic VLAN by entering the **switchport access vlan dynamic** interface configuration command on it, the switch might reload when it processes ARP requests on the port.

The workaround is to configure static VLANs for these ports.

- CSCtq48441 (Catalyst Switches ME-3400 and ME-3400E)

  The **ip sla** global configuration command does not function in the command line interface.

  There is no workaround.

- CSCtr53304 (Catalyst Switch ME-3400E)

  When sending data with large packet sizes, bandwidth is not allocated properly. Sometimes, certain classes of service are not allocated any bandwidth regardless of being adequately provisioned by the **bandwidth** global configuration command. This limitation occurs at the application-specific integrated circuit (ASIC) level.

  The workaround is to configure classes in a descending order of bandwidth. (For example, configure a class with a bandwidth value of 30000 before configuring a class with a bandwidth value of 25000.) This workaround applies when only one working policy map is configured in the switch or when the working policy map is configured before other policy maps. For other cases, there is no workaround.

Caveats Resolved in Cisco IOS Release 12.2(58)SE1

- CSCtg00542

  A Link Aggregation Control Protocol (LACP) bundle takes up to 70 seconds to form when NetFlow sampling is enabled.

  The workaround is to disable NetFlow sampling.

- CSCtg11547

  When you configure a switch to send messages to a syslog server in a VPN Routing and Forwarding (VRF) instance, the messages are not sent to the server.

  The workaround is to remove the VRF configuration.

- CSCtg71149

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

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

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

- CSCth53532

  When you configure priority policing on a ME 3400E or ME 3400 switch, the allocated bandwidth does not reflect the actual traffic rate.

  Use one of these workarounds:

  Configure an explicit bandwidth percentage in the class-default or other configured class.

  Change the priority configuration from a percentage to an absolute value.

- CSCth79300

  When an access control list (ACL) that permits only bidirectional forwarding detection (BFD) and border gateway protocol (BGP) packets is applied to an interface on a switch running Cisco IOS Release 12.2(54)SE, the BFD session goes down but the BGP peer stays up.

  The workaround is to remove the ACL from the interface.

- CSCti26354 (ME 3400 switch)

  When a switch running Cisco IOS Release 12.2(53)SE, 12.2(54)SE, or 12.2(55)SE is connected to another switch through a 1000BASE-EX SFP (GLC-EX-SMD) module port, and the link is error disabled, this message appears:

  ```
  %PHY-4-SFP_NOT_SUPPORTED: The SFP in Gi0/1 is not supported
  ```

  There is no workaround.

- CSCti62848

  The switch fails when you configure a new aggregate policer in a class and the policer has a name that is longer than the name of the existing aggregate policer in that class.

  The workaround is to clear the existing aggregate policer before attaching the new one or to use a name for the new aggregate policer that is shorter than the name of the existing aggregate policer in that class.

- CSCti78365

  The config.text.backup file is present after the switch is restored to the factory defaults.

  There is no workaround.

- CSCti95834

  When you enter the **ipv6 traffic-filter** interface configuration command, it might not filter traffic as expected, and it might allow traffic to pass through.

  There is no workaround.

- CSCtj01016 (ME 3400E switch)

  QoS shaper accuracy varies with the configured interface speed and packet size, partially because QoS port shaper calculations account for interpacket gap, while QoS queue shaper calculations do not. In Cisco IOS Release 12.2(55)SE3 and 12.2(58)SE, the port shaper is optimized for 512 byte-packets to account for various interface speeds and configuration values. However, accuracy can still vary for other packet sizes because of interpacket gap inconsistencies.

  The accuracy has been improved across different configuration values and interface speeds. However, there is no workaround for the inaccuracy introduced due to interpacket gaps for packet sizes other than 512 bytes. You should adjust QoS configuration to account for the differences between the port shaper and queue shaper.

- CSCtj03875

  When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.

  There is no workaround.

- CSCtj10693

  When you enter the **permit any any** access-list configuration command, it matches most of the MAC addresses, but it cannot match and police some MAC addresses.

  There is no workaround.

- CSCtj75471

  When a spanning-tree bridge protocol data unit (BPDU) is received on an 802.1Q trunk port and has a VLAN ID is greater than or equal to 4095, the spanning-tree lookup process fails.

  There is no workaround.

- CSCtj88307

  When you enter the **default interface**, **switchport**, or **no switchport** interface configuration command on the switch, this message appears: *EMAC phy access error, port 0, retrying.....*

  There is no workaround.

- CSCtk11275

  On a switch running Cisco IOS Release 12.2(55)SE with the **parser config cache interface** global configuration command in the configuration, when you use the CISCO-MAC-NOTIFICATION-MIB to enable the SNMP MAC address notification trap, the trap is enabled, but the trap setting does not appear in the switch configuration.

  The workaround is to remove the **parser config cache interface** command from the configuration.

- CSCtk76719

  A switch running Cisco IOS Release 12.2(55)SE that has oversubscribed or congested Resilient Ethernet Protocol (REP) links might experience REP instabilities and display this error message:

  ```
  %REP-4-LINKSTATUS: GigabitEthernet0/12 (segment 1) is non-operational due to neighbor
  not responding
  ```

  There is no workaround.

- CSCtl42740

  When 802.1x MAC authentication bypass with multidomain authentication and critical VLAN are enabled on an interface on a switch running Cisco IOS Release 12.2(53)SE or later, if the switch loses connectivity with the AAA server, the switch might experience high CPU usage and show these messages:

  ```
  AUTH-EVENT (Gi0/15) Received clear security violation
  AUTH-EVENT (Gi0/15) dot1x_is_mab_interested_in_mac: Still waiting for a MAC on port
  GigabitEthernet0/15
  ```

  There is no workaround.

- CSCto62631

  A switch running Cisco IOS Release 12.2(58)SE might reload if:

  - SSH version 2 is configured on the switch, and
  - a customized login banner was configured by using the **banner login** *message* global configuration command

  Use one of these workarounds:

  - Disable the login banner by entering the **no login banner** command.
  - Disable SSH on the switch.
  - Downgrade to a software version prior to Cisco IOS Release 12.2(58)SE.

Documentation Updates

Note The "Supported MIBs" appendix is no longer in the software configuration guide. To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

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 System Message Guide

New System Messages

Error Message `IP-3-SBINIT: Error initializing [chars] subblock data structure. [chars]`

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

Error Message `AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]`

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation All available authentication methods have been tried. The first [chars] is the client identifier, the second [chars]s is the interface for the client, and the third [chars] is the session ID.

Recommended Action No action is required.

Modified System Messages

Error Message `AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]`

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message `AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])`

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

Deleted System Messages

Error Message `IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: [inet], hw: [enet] by hw: [enet]\n", MSGDEF_LIMIT_FAST`

Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that triggered this message.

Recommended Action Change the IP address of one of the two systems.

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 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

User documentation in HTML format includes the latest documentation updates and might be more current than the complete book PDF available on Cisco.com.

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:
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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

© 2011, 2012 Cisco Systems, Inc. All rights reserved.