Release Notes for Cisco Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter, Cisco IOS Release 12.2(55)SE

August 12, 2010

Cisco IOS Release 12.2(55)SE runs only on Catalyst Switch Module 3110G, 3110X, and 3012.

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

- If you are installing a new switch module, see the Cisco IOS release label on the rear panel of your switch module.
- If your switch module is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 4.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 5.

You can download the switch module software from these sites (registered Cisco.com users with a login password):

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

http://www-304.ibm.com/systems/support/supportsite.wss/selectproduct?brandind=5000020&taskind=2

For the complete list of Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter documentation, see the "Related Documentation" section on page 31.

Contents

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

System Requirements

Hardware Supported

Table 1 Catalyst Switch Module Supported Hardware

Switch Module Hardware	Description	Supported by Minimum Cisco IOS Release
Catalyst Switch Module 3110G	4 external 10/100/1000BASE-T Ethernet ports, 14 internal 1000BASE-X Ethernet downlink ports, 1 internal 100BASE-T Ethernet management port, 2 StackWise Plus ports	Cisco IOS Release 12.2(40)EX2
Catalyst Switch Module 3110X	1 external 10-Gigabit Ethernet module slot, 14 internal 1000BASE-X Ethernet downlink ports, 1 internal 100BASE-T Ethernet management port, 2 StackWise Plus ports **Note** The Cisco TwinGig Converter Module (model CVR-X2-SFP) is supported in Cisco IOS Release 12.2(52)SE or later.	Cisco IOS Release 12.2(40)EX2
Catalyst Switch Module 3012	4 external 10/100/1000BASE-T Ethernet ports, 14 internal 1000BASE-X Ethernet downlink ports, 1 internal 100BASE-T Ethernet management port	Cisco IOS Release 12.2(40)EX2
Cisco X2 transceiver modules	X2-10GB-SR X2-10GB-LX4 X2-10GB-CX4 X2-10GB-LR X2-10GB-LRM **Note** Cisco X2 transceiver modules are only supported on the Catalyst Switch Module CBS3110X.	12.2(40)EX1 12.2(46)SE

Table 1 Catalyst Switch Module Supported Hardware (continued)

Switch Module Hardware	Description	Supported by Minimum Cisco IOS Release
SFP modules[1]	GLC-T GLC-SX-MM GLC-LH-SM **Note** SFP Modules require the use of TwinGig adapter (CVR-X2-SFP).	12.2(52)SE
Supports OneX (CVR-X2-SFP10G) and these SFP+ modules (For the Catalyst Switch Modules 3110G and 3110X)	SFP-10G-SR SFP-10G-LR SFP-10G-LRM Only version 02 or later CX1[2] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	12.2(53)SE

1. SFP = small form-factor pluggable
2. The CX1 cables are used with the OneX converters.

Table 2 lists the IBM BladeCenter supported blade enclosures. The switch module is for use only in listed IBM BladeCenter products.

Table 2 IBM BladeCenter Supported Switch Modules

Model	Switch Module 3110G	Switch Module 3110X	Switch Module 3012
BladeCenter E (BC-E)	Yes	Yes	Yes
BladeCenter T (BC-T)	Yes	Yes	Yes
BladeCenter H (BC-H)	Yes	Yes	Yes
BladeCenter HT (BCH-T)[1]	Yes	Yes	Yes
BladeCenter S (BC-S)	No	No	Yes
BladeCenter Multi-switch Interconnect Module (MSIM)	Yes[2]	Yes[2]	Yes

1. The Cisco Catalyst Switch modules are not supported in the MSIM-T module.
2. The advanced Management Module (aMM) firmware must use Version 1.42i or higher.

Device Manager System Requirements

Hardware Requirements

Table 3 Minimum Hardware Requirements

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

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

Software Requirements

These are the supported operating systems and browsers for the device manager:

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 5.5, 6.0, 7.0, Firefox 1.5, 2.0 or later.

The device manager verifies the browser version when starting a session, and it does not require a plug-in.

CNA Compatibility

Cisco IOS Release 12.2(40)EX2 and later is only compatible with Cisco Network Assistant 5.0 and later. You can download Network Assistant from this URL:

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

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Module Software

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

- "Finding the Software Version and Feature Set" section on page 4
- "Deciding Which Files to Use" section on page 5
- "Upgrading a Switch Module by Using the Device Manager or Network Assistant" section on page 6
- "Upgrading a Switch Module by Using the CLI" section on page 6
- "Recovering from a Software Failure" section on page 7

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board flash device (flash:).

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

Note Although the **show version** output always shows the software image running on the switch module, the model name at the end of this display is the factory configuration (IP base feature set or IP services feature set). It does not change if you upgrade the software license.

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

Deciding Which Files to Use

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

Table 4 Cisco IOS Software Image Files for Catalyst Switch Modules

Filename	Description
cbs31x0-universal-tar.122-55.SE.tar	Catalyst switch module universal image and device manager files. This image has all the supported features that are enabled by the software license installed on the switch module.
cbs31x0-universalk9-tar.122-55.SE.tar	Catalyst switch module universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.

The universal software images support multiple feature sets. Use the software activation feature to deploy a software license and to enable a specific feature set. For information about software activation, see the *Cisco Software Activation for IBM* document on Cisco.com:

http://www.cisco.com/en/US/products/ps8741/products_installation_and_configuration_guides_list.html

Archiving Software Images

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

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

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

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

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

You can also configure the switch module as a TFTP server to copy files from one switch module 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 Module by Using the Device Manager or Network Assistant

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

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

Upgrading a Switch Module by Using the CLI

This procedure is for copying the combined tar file to the switch module. You copy the file to the switch module from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, follow these steps:

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

Step 2 Download the software image file:

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

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

b. Navigate to **Switches > Blade Switches.**

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, see Appendix B in the software configuration guide for this release.

Step 4 Log into the switch module through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

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

For more information about assigning an IP address and default gateway to the switch module, see the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch module. If you are installing the same version of software that is currently on the switch module, 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 module:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/cbs31x0-universal-tar.image-name.tar
```

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

Recovering from a Software Failure

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

Installation Notes

You can assign IP information to your switch module by using the IBM advanced Management Module software and the switch module device manager Express Setup program, as described in the switch module getting started guide.

New Software Features

- Auto-QoS enhancements that add automatic configuration classification of traffic flow from video devices, such as the Cisco Telepresence System and Cisco Surveillance Camera.
- Support for CDP and LLDP enhancements for exchanging location information with video end points for dynamic location-based content distribution from servers.
- Support for dynamic creation or attachment of an auth-default ACL on a port that has no configured static ACLs configured.

- Support for VLAN assignment on a port configured for multi-auth mode. The RADIUS server assigns a VLAN to the first host to authenticate on the port, and subsequent hosts use the same VLAN. Voice VLAN assignment is supported for one IP phone.
- Support for the Security Group Tag (SCT) Exchange Protocol (SXP) component of Cisco TrustSec, a security architecture using authentication, encryption, and access control.
- AAA guarantee-first support for enabling or disabling system accounting as the first record.
- An option to suppress verbose 802.1x, authentication manager, and MAC authentication bypass syslog messages.
- Support for Embedded Event Manager (EEM) in the IP base image.
- Support for QoS class-default policy placement.
- The IP Base image supports OSPF for routed access to enable customers to extend Layer 3 routing capabilities to the access or wiring closet. The IP services image is required if you need multiple OSPFv2 and OSPFv3 instances without route restrictions.
- MAC move to allow hosts (including the hosts connected to an IP phone) to move across ports within the same switch without any restrictions to enable mobility. With MAC move, the switch treats the reappearance of the same MAC address on another port as a completely new MAC address.

  MAC replace can be configured so that when a host disconnects from a port without ending its session, the session can be ended and the authentication sequence reset when a new MAC address connects to the port.
- Support for increasing the NVRAM buffer size for saving large configuration files.
- ARP tracking probe enhancement to specify a source IP address for a VLAN.

Minimum Cisco IOS Release for Major Features

Table 5 lists the minimum software release (after the first release) required to support the major features of the Catalyst Switch Module 3110G, 3110X, and 3012. Features not listed are supported in all releases.

Table 5 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Module Support
Auto-QoS enhancements	12.2(55)SE	3110G, 3110X, and 3012
Port ACL improvements	12.2(55)SE	3110G, 3110X, and 3012
CDP location enhancements	12.2(55)SE	3110G, 3110X, and 3012
Multi-authentication with VLAN assignment	12.2(55)SE	3110G, 3110X, and 3012
Cisco TrustSec	12.2(55)SE	3110G, 3110X, and 3012
MAC replace to end a session when a host disconnects from a port.	12.2(55)SE	3110G, 3110X, and 3012
VRF Aware RADIUS	12.2(53)SE	3110G, 3110X, and 3012
Full QoS support for IPv6 traffic.	12.2(52)SE	3110G, 3110X, and 3012
Cisco Medianet to enable intelligent services in the network infrastructure.	12.2(52)SE	3110G, 3110X, and 3012
Support for IP source guard on static hosts.	12.2(52)SE	3110G, 3110X, and 3012

Table 5 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Module Support
RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated.	12.2(52)SE	3110G, 3110X, and 3012
IEEE 802.1x User Distribution to allow deployments with multiple VLANs.	12.2(52)SE	3110G, 3110X, and 3012
Support for critical VLAN with multiple-host authentication.	12.2(52)SE	3110G, 3110X, and 3012
Customizable web authentication enhancement.	12.2(52)SE	3110G, 3110X, and 3012
Support for Network Edge Access Topology (NEAT).	12.2(52)SE	3110G, 3110X, and 3012
VLAN-ID based MAC authentication.	12.2(52)SE	3110G, 3110X, and 3012
MAC move to allow hosts to move across ports within the same switch.	12.2(52)SE	3110G, 3110X, and 3012
Support for including a hostname in the option 12 field of DHCPDISCOVER packets.	12.2(52)SE	3110G, 3110X, and 3012
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	3110G, 3110X, and 3012
Support for VTP version 3.	12.2(52)SE	3110G, 3110X, and 3012
Network Edge Access Topology (NEAT) with 802.1x	12.2(50)SE	3110G, 3110X, and 3012
IEEE 802.1x with open access	12.2(50)SE	3110G, 3110X, and 3012
IEEE 802.1x authentication with downloadable ACLs and redirect URLs	12.2(50)SE	3110G, 3110X, and 3012
Flexible-authentication sequencing of authentication methods	12.2(50)SE	3110G, 3110X, and 3012
Multiple-user authentication on an 802.1x-enabled port.	12.2(50)SE	3110G, 3110X, and 3012
Cisco EnergyWise	12.2(50)SE	3110G, 3110X, and 3012
Wired location service	12.2(50)SE	3110G, 3110X, and 3012
Intermediate System-to-Intermediate System (IS-IS) routing	12.2(50)SE	3110G, 3110X, and 3012
Stack troubleshooting enhancements	12.2(50)SE	3110G nd 3110X
CPU utilization threshold trap	12.2(50)SE	3110G, 3110X, and 3012
Embedded Event Manager Version 2.4	12.2(50)SE	3110G, 3110X, and 3012
LLDP-MED network-policy profile time, length, value (TLV) for creating a profile for voice and voice-signalling	12.2(50)SE	3110G, 3110X, and 3012
RADIUS server load balancing	12.2(50)SE	3110G, 3110X, and 3012
Auto Smartports Cisco-default and user-defined macros	12.2(50)SE	3110G, 3110X, and 3012
Support for IPv6 features in the IP base and IP services feature sets	12.2(50)SE	3110G, 3110X, and 3012
Voice aware IEEE 802.1x and MAC authentication bypass (MAB) security violation	12.2(46)SE	3110G, 3110X, and 3012
Local web authentication banner	12.2(46)SE	3110G, 3110X, and 3012
Support for HSRP Version 2 (HSRPv2)	12.2(46)SE	3110G and 3110X
Disabling MAC address learning on a VLAN	12.2(46)SE	3110G, 3110X, and 3012
PAgP Interaction with Virtual Switches and Dual-Active Detection.	12.2(46)SE	3110G, 3110X, and 3012

Table 5 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Module Support
Support for rehosting a software license and for using an embedded evaluation software license	12.2(46)SE	3110G, 3110X, and 3012
DHCP server port-based address allocation.	12.2(46)SE	3110G, 3110X, and 3012
HSRP for IPv6	12.2(46)SE	3110G and 3110X
DHCP for IPv6 relay, client, server address assignment and prefix delegation	12.2(46)SE	3110G and 3110X
IPv6 default router preference (DRP).	12.2(46)SE	3110G, 3110X, and 3012
Generic message authentication support with the SSH Protocol and compliance with RFC 4256.	12.2(46)SE	3110G, 3110X, and 3012

Limitations and Restrictions

You should review this section before you begin working with the switch module. 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 module hardware or software.

- "Cisco IOS Limitations" section on page 10
- "Device Manager Limitations" section on page 15
- "IBM BladeCenter Advanced Management Module Limitations" section on page 15
- "SoL and cKVM" section on page 15

Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst Switch Module 3110G, 3110X, and 3012:

- "Access Control List" section on page 11
- "Address Resolution Protocol" section on page 11
- "Cisco X2 Transceiver Modules" section on page 11
- "Configuration" section on page 11
- "HSRP" section on page 12
- "IEEE 802.1x Authentication" section on page 12
- "Multicasting" section on page 13
- "Quality of Service (QoS)" section on page 14
- "RADIUS" section on page 14
- "Routing" section on page 15
- "SPAN and RSPAN" section on page 15
- "SPAN and RSPAN" section on page 15

Access Control List

- When a MAC access list is used to block packets from a specific source MAC address, that MAC address is entered in the switch module MAC-address table.

  The workaround is to block traffic from the specific MAC address by using the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command. (CSCse73823)

Address Resolution Protocol

- The switch module might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem.(CSCse06827))

Cisco X2 Transceiver Modules

- Switch modules with the Cisco X2-10GB-LX4 transceiver modules with a version identification number before V03 might intermittently fail. The workaround is to use Cisco X2-10GB-LX4 transceiver modules with a version identification number of V03 or later. (CSCsh60076)
- When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the **show controllers ethernet-controller tengigabitethernet** privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior, based IEEE 802.3ae. (CSCsd47344)

Configuration

- When an excessive number (more than 100 packets per second) of Address Resolution Protocol (ARP) packets are sent to a Network Admission Control (NAC) Layer 2 IP-configured member port, a switch module might display a message similar to this:

  ```
  PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism: type 0, class
  51, max_msg 128, total throttled 984323
  -Traceback= 6625EC 5DB4C0 5DAA98 55CA80 A2F2E0 A268D8
  ```

  No workaround is necessary. Under normal conditions, the switch module generates this notification when snooping the next ARP packet. (CSCse47548)
- When there is a VLAN with protected ports configured in a fallback bridge group, packets might not be forwarded between the protected ports.

  The workaround is to not configure VLANs with protected ports as part of a fallback bridge group. (CSCsg40322)
- When a switch module port configuration is set at 10 Mb/s and half duplex, sometimes the port does not send in one direction until the port traffic is stopped and then restarted. You can detect the condition by using the **show controller ethernet-controller** or the **show interfaces** privileged EXEC commands.

  The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the **shutdown** interface configuration command followed by the **no shutdown** command on the interface. (CSCsh04301)

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

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

- (Only Catalyst Switch Module 3110G and 3012) These privileged EXEC commands incorrectly display the internal, nonconfigurable Gigabit Ethernet interfaces n/0/19 and n/0/20.

```
show mls qos interface
show mls qos interface buffers
show mls qos interface policers
show mls qos interface queueing
show mls qos interface statistics
show mac access-group
show controllers ethernet-controller
show interfaces Gin/0/19 [all options]
show idb all
```

  There is no workaround. (CSCsk51772)

- If there is large-volume bidirectional traffic on the switch module Fa0 management interface, some packets might be dropped because of CPU limitations. This is not a likely occurrence because the Fa0 interface typically does not send or receive large-volume traffic.

  There is no workaround. (CSCso35380)

- (Only Catalyst Switch Module 3110X) If you configure port security on Gigabit Ethernet interface n/0/14, the switch module software does not accept the command.

  There is no workaround. (CSCso75068)

- If you enter the **show tech-support** privileged EXEC command after you enter the **remote command** {**all** | *stack-member-number*} privileged EXEC command, the complete output does not appear.

  The workaround is to use the **session** *stack-member-number* privileged EXEC command. (CSCsz38090)

HSRP

- When the switch stack is in the HSRP active state and a master changeover occurs, you cannot ping the stack by using an HSRP virtual IP address.

  There is no workaround.(CSCth00938)

IEEE 802.1x Authentication

- (Catalyst switch module 3110X only) If you try to configure IEEE 802.1x Authentication on Gigabit Ethernet interface n/0/14, the switch module software does not accept the command. The CLI for IEEE 802.1x is disabled on Gigabit Ethernet interface n/0/14.

- If a supplicant using a Marvel Yukon network interface card (NIC) is connected an IEEE 802.1x-authorized port in multihost mode, the extra MAC address of 0c00.0000.0000 appears in the MAC address table.

  Use one of these workarounds (CSCsd90495):

  – Configure the port for single-host mode to prevent the extra MAC address from appearing in the MAC address table.

  – Replace the NIC with a new card.

- When MAC authentication bypass is configured to use Extensible Authentication Protocol (EAP) for authorization and critical authentication is configured to assign a critical port to an access VLAN:

  – If the connected device is supposed to be unauthorized, the connected device might be authorized on the VLAN that is assigned to the critical port instead of to a guest VLAN.

  – If the device is supposed to be authorized, it is authorized on the VLAN that is assigned to the critical port.

  Use one of these workarounds (CSCse04534):

  – Configure MAC authentication bypass to not use EAP.

  – Define your network access profiles to not use MAC authentication bypass. For more information, see the Cisco Access Control Server (ACS) documentation.

Multicasting

- Multicast packets with a time-to-live (TTL) value of 0 or 1 are flooded in the incoming VLAN when all of these conditions are met:

  – Multicast routing is enabled in the VLAN.

  – The source IP address of the packet belongs to the directly connected network.

  – The TTL value is either 0 or 1.

  The workaround is to not generate multicast packets with a TTL value of 0 or 1 or to disable multicast routing in the VLAN. (CSCeh21660)

- Multicast packets denied by the multicast boundary access list are flooded in the incoming VLAN when all of these conditions are met:

  – Multicast routing is enabled in the VLAN.

  – The source IP address of the multicast packet belongs to a directly connected network.

  – The packet is denied by the IP multicast boundary access-list configured on the VLAN.

  There is no workaround. (CSCei08359)

- Reverse path forwarding (RPF) failed multicast traffic might cause a flood of Protocol Independent Multicast (PIM) messages in the VLAN when a packet source IP address is not reachable.

  The workaround is to not send RPF-failed multicast traffic, or make sure that the source IP address of the RPF-failed packet is reachable. (CSCsd28944)

- If you use the **clear ip mroute** privileged EXEC command when multicast packets are present, it might cause temporary flooding of incoming multicast traffic in the VLAN.

  There is no workaround. (CSCsd45753)

- When you configure the **ip igmp max-groups** *number* and **ip igmp max-groups action replace** interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value. No workaround is necessary. The problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)

Quality of Service (QoS)

- When QoS is enabled and the egress port receives pause frames at the line rate, the port cannot send packets.

  There is no workaround. (CSCeh18677)

- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.

  There is no workaround. (CSCsc63334)

- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch module rejects the configuration. The VLAN-level policy map is removed from the interface.

  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)

- If the ingress queue has low buffer settings and the switch module sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.

  There is no workaround. (CSCsd72001)

- When you use the **srr-queue bandwidth limit** interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy improves when the packet size is greater than 512 bytes.

  There is no workaround. (CSCsg79627)

- If QoS is enabled on a switch and the switch has a high volume of incoming packets with a maximum transmission unit (MTU) size greater than 1512 bytes, the switch might reload.

  Use one of these workarounds:

  – Use the default buffer size.

  – Use the **mls qos queue-set output** *qset-id* **buffers** *allocation1 ... allocation4* global configuration command to allocate the buffer size. The buffer space for each queue must be at least 10 percent. (CSCsx69718)

- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

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

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

RADIUS

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

  There is no workaround. (CSCta05071)

Routing

- When the PBR is enabled and QoS is enabled with DSCP settings, the CPU usage might be high if traffic is sent to unknown destinations.

  The workaround is to not send traffic to unknown destinations. (CSCse97660)

SPAN and RSPAN

- When egress SPAN is running on a 10-Gigabit Ethernet port, only about 12 percent of the egress traffic is monitored.

  There is no workaround. This is a hardware limitation. (CSCei10129)

Stacking

- Creating a mixed switch stack with a Catalyst Switch Module 3110, a Catalyst Switch Module 3120, or a Catalyst Switch Module 3130 produces unpredictable behavior and could cause a system failure. Because the switch module software does not detect this type of configuration, it allows a stack of this type.

  There is no workaround. This is not a supported configuration. (CSCsj44478)

Device Manager Limitations

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

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

IBM BladeCenter Advanced Management Module Limitations

- When a switch module is installed in a BC-HT chassis with the ISL Interposer, the switch module incorrectly reports that it is installed in a BC-T chassis and that it provides 8 server ports and no ISL ports. When it is installed with the non-ISL Interposers, the switch module incorrectly reports that it is installed in a BC-H chassis and that it provides 14 server ports.

  See the IBM Retain database for more information.

SoL and cKVM

Serial over LAN (SoL) can be used to manage remote servers through the command-line interface (CLI) over a Telnet or Secure Shell (SSH) connection. A systems management controller is on each server, and the server serial ports are connected through an IP network. SoL is available even with no operating system on the server.

With concurrent Keyboard, Video, and Mouse (cKVM) support, an enhancement of standard KVM, you can access all servers at the same time. cKVM also uses systems management controller to send traffic.

IBM BladeCenter SoL and cKVM traffic is encapsulated and sent on one of the chassis switch modules via VLAN 4095 to the IBM management module. This traffic is sent separately from the server traffic. The IBM BladeCenter servers support VLAN 4095, SoL, and cKVM.

These limitations apply to all server facing ports on the Cisco Catalyst Switch Module CBS3110X, CBS3110G, and CBS3012:

- The protected port feature on the switch and the SoL and cKVM features on the server are mutually exclusive. If the protected port feature is enabled on a port and traffic from that port is forwarded to uplink ports, SoL and cKVM traffic is not forwarded from the server serial port to the port. This applies to all VLANs on the switch, including VLAN 4095.

  There is no workaround

- If you enable port security on a port, it does not respond to or forward SoL and cKVM packets.

  There is no workaround.

- During IEEE 802.1x authentication, the switch assigns the port to a VLAN on which traffic is forwarded. The SoL and cKVM traffic is blocked on the port because the Cisco IOS software does not support VLAN 4095 directly.

  There is no workaround.

- If the server port is configured as a router port, SoL and cKVM traffic is not forwarded through Layer 2 switches to the AMM and the servers cannot be managed remotely. SoL and cKVM traffic is forwarded only if the servers facing port are configured as switch ports.

  There is no workaround.

- If you enable an EtherChannel on the server facing ports, the SoL traffic might not forwarded to the correct NIC.

  The workaround is to configure the proper load-balancing method that always forwards the SoL traffic to the active NIC.

- If a port access control list (ACL) is applied to the port and SoL and cKVM traffic must be permitted, configure a permit access control entry (ACE) for the systems management controller. This information is available on the Advanced Management Module (AMM) interface.

- In **show** privileged EXEC command output for the switch port and the server, the counters (number of packets and bytes) for received and sent server traffic are less than the counters for received and sent port traffic. The **show** command output on the switch has the aggregate counters of the server traffic and the remote management traffic.

On the Catalyst Switch Module 3110X only, port 14 is the collector port receiving SoL and cKVM traffic. In addition to the previous limitations, these also apply to this port:

- If you configure port 14 as a SPAN destination port, the switch cannot receive SoL and cKVM traffic.
- Due to the nature of the collector port, the Cisco IOS CLI commands for protected port, port security, and 802.1x authentication are disabled on port 14.

Important Notes

Cisco IOS Notes

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

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

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

Device Manager Notes

- You cannot create and manage switch module clusters through the device manager. To create and manage switch module clusters, use the CLI or Cisco Network Assistant.
- When the switch module is running a localized version of the device manager, the switch module displays settings and status only in English letters. Input entries on the switch module can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.
- We recommend this browser setting to reduce the time needed to display the device manager from Microsoft Internet Explorer.

  From Microsoft Internet Explorer:

  1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the "Temporary Internet files" area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch module. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

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

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

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

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

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

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

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

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

Open Caveats

- CSCsy33664

  On the Catalyst Switch Module 3012, the **license boot level** global configuration command shows **ipbase** and **ipservices** as available keywords. The **ipservices** keyword is not supported. The switch supports only the IP base image.

  There is no workaround.

- CSCta72141

  The bootloader label is incorrect and displays “CISCO DEVELOPMENT TEST VERSION.” However, the actual bootloader software is the correct version with the correct functionality.

  There is no workaround. It does not impact functionality.

- CSCtf34659

  You cannot ping the Ethernet management port interface (Fa0) on the switch after you configure an IP address on the VLAN 1 interface.

  There is no workaround.

- 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.

- CSCth88306

  This message appears after inserting the CVR-X2-SFP converter module and the X2-10GB-SR transceiver modules in the10-Gigabit slots of the Catalyst 3750-E and 3560-E switches:

  ```
  %GBIC_SECURITY_CRYPT-4-VN_DATA_CRC_ERROR: GBIC in port Te1/0/1 has bad crc
  ```

  There is no workaround.

Resolved Caveats

- CSCsg28558

  Cisco X2-10GB-CX4 transceiver modules with a version identification number lower than V03 might be difficult to install because of a size discrepancy.

  The workaround is to use modules with a version identification number of V03 or later.

- CSCsg91027

  When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU usage. CPU usage can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch module operates and could cause problems such as STP convergence delay.

  High CPU usage can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

  Use one of these workarounds:

  - Disable logging to the console.
  - Rate-limit logging messages to the console.
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces.

- CSCsu31853

  The buffer space of a switch running TCP applications is full while the TCP sessions are in the TIME_WAIT state. Buffer space becomes available after the TCP session the closed.

  There is no workaround.

- 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.

- CSCtb58779

  When a switch is low on memory (less than 256 MB), it can reload and display a SYS-2-WATCHDOG error.

  There is no workaround. Enter the **show memory debug leak** privileged EXEC command to check for signs of a memory leak and address these symptoms.

- CSCtc02635

  On switches running Cisco IOS release 12.2(50)SE3 running MAC authentication bypass with multidomain authentication (MDA), IP phones connected to a port might not be able to regain network connectivity in the VOICE domain if the session times out and all RADIUS servers are unreachable.

  There is no workaround.

- CSCtc38519 (3110G and 3012 switches)

  Attempts to restore factory default settings from the advanced Management Module (aMM) web interface fail. After the switch restarts, the configurations are not erased and restored to their factory default settings. Switches that run Cisco IOS Release 12.2(50)SE or Release 12.2(52)SE are affected.

  Workaround: Enter the **write erase** privileged EXEC command from the switch console, do not save the configuration from the switch console, and then restart the switch.

- CSCtc57809

  Switches running Cisco IOS Release 12.2(52)SE might reload after you enter the **no mac address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id* global configuration command if the interface is up and the MAC address was dynamically learned before it was changed to static.

  Use one of these workarounds:

  – Clear the dynamic MAC address table when configuring static MAC addresses as in this example:

  ```
  Switch(config)# no mac address-table learning vlan vlan_id
  Switch(config)# clear mac-address-table dynamic address mac_address
  Switch(config)# mac address-table static mac_address vlan vlan_id interface interface_id
  Switch(config)# mac address-table learning vlan vlan_id
  ```

  – Downgrade to Cisco IOS Release 12.2(50)SE.

  – Upgrade to Cisco IOS Release 12.2(53)SE if available.

- CSCtc77969

  When PAgP or LACP EtherChannels are configured on a switch and the stack reloads, entering a **show interface** or **show etherchannel summary** privileged EXEC command when the stack comes up can cause the console to lock up.

  There is no workaround.

- CSCtd02006

  After a 10-Gigabit Ethernet interface in an X2-10GB-SR module is down and the switch is restarted, the **show inventory** command output shows the module as not present.

The workaround is to reinstall the X2-10GB-SR module or to restart the switch.

- CSCtd29049

  A switch that has at least one trunk port configured might fail when you configure more than 950 VLANS by using the **vlan** *vlan-id* global configuration command.

  There is no workaround.

- CSCte00827

  When a port that is configured for Switched Port Analyzer (SPAN) goes up and down, a memory leak occurs in the 'hpm main' process.

  There is no workaround.

- CSCte72365

  After a software upgrade from Cisco IOS Release 12.2(52)SE to Cisco IOS Release 12.2(53)SE, EIGRP hello packets are flooded on access ports belonging to another subnet. The same result occurs when you initiate ping requests to the broadcast address of other subnets. This results in *Not on common subnet* errors on the other side of the link.

  The workaround is to downgrade to 12.2(52)SE

- CSCte94620

  After you apply an ACL, these messages appear:

  ```
  %IPACCESS-4-INVALIDACL: Invalid ACL field: Acl number is 0
  %IPACCESS-4-INVALIDACL: Invalid ACL field: Acl type is 145
  ```

  There is no workaround.

- CSCte99016 (3110 switch)

  When two blade switches in a blade server are running Cisco IOS release 12.2(53)SE, with no stack cable connection between them, if you enter the **no shutdown** interface command on gigabitethernet ports 1/0/17 and 1/0/18, the output of the **show running-config** or **show interface** privileged EXEC command shows the ports to be down.

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

- CSCte99650

  You can see this error message on the switch message logs:

  %PLATFORM_ENV-1-TEMP: Abnormal temperature detected

  However, when you enter the **show env all** privileged EXEC command, the temperature value shows it to be well within the limits.

  There is no workaround.

- CSCtf17223

  If you try to access the Web-based device manager from the IBM AMM, the switch incorrectly reports to the IBM blade center chassis that it supports only https and does not support http.

  When you access device manager from the AMM, the URL link is always https://. The workaround is to manually change it to http:// in the browser.

- CSCtf33948

  A PC in 802.1x or MDA mode is connected to an IP phone and connected to a MDA-enabled switch port. After the PC and phone are authenticated on the port, the PC is down. The port does not automatically reauthenticate the PC.

  There is no workaround.

- CSCtf78276

  A switch running Cisco IOS Release 12.2(53)SE1 stops when IEEE 802.1x authentication is enabled.

  The workaround is to apply a VLAN that the RADIUS server assigned to the switch.

- CSCtf19991

  If the RADIUS authentication server is unavailable and inaccessible authentication bypass is enabled, the switch grants the client access to the network by putting the connected port in the critical-authentication state in the RADIUS-configured or the user-specified access VLAN. After the server is available, the client is not reinitalized and moved out of the critical VLAN.

  There is no workaround.

- CSCtg14607

  Replacing the power module can cause the advanced management module (AMM) to fail to connect with the switches.

  The workaround is to restart the AMM.

- CSCtg26941

  Multidomain authentication (MDA) with guest VLAN or MAC authentication bypass (MAB) as a fallback method is enabled on a switch running Cisco IOS Release 12.2(53)SE. When a non-802.1x client is connected to a IP phone and the phone connected to a switch port shuts down and then restarts, the client MAC address status is *drop* in the MAC address table. It takes 5 minutes for the client to access the network.

  The workaround is to use another software release, such as Cisco IOS Release 12.2(44)SE2.

- CSCtg47738

  This error message is displayed after copying a configuration file to the running configuration file fails:

  ```
  %Error opening system:/running-config (No such file or directory)
  ```

  The output of the **dir system:/** EXEC command also does not show a running configuration file.

  The workaround is to reload the switch.

- CSCtg88183

  The switch internally uses the **mac-address-table static** *mac-address* deprecated global configuration command to configure the MAC address on the Ethernet management port (Fa0).

  The workaround is to use the correct version of the command: **mac address-table static** *mac-address*.

- CSCth18118 (3110 switch)

  When VTP pruning is enabled in a VTP domain, the switch in VTP server mode sends advertisements to neighboring switches. If the VTP and VLAN configuration for neighboring ports is not updated, VLANs on those ports can be pruned, causing a network traffic outage.

  The workaround is to disable VTP pruning.

- CSCti04980

  After you upgrade the switch software to Cisco IOS Release 12.2(55)SE, enhanced auto-QoS commands are generated when

  – auto-QoS is enabled on an interface

  and

  – **mls qos** command is not enabled on the switch

  If the **mls qos** command was already enabled on the switch, enhanced auto-QoS commands are generated only when you configure one of these commands:

  – **auto qos classify** [**police**]

  – **auto qos trust** {**cos** | **dscp**}

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

  Cisco IOS Release 12.2(55)SE supports implicit and explicit migration to enhanced auto-QoS configurations.

  Implicit migration to enhanced auto-QoS occurs on a switch running legacy auto-QoS when you configure the **auto qos video**, **auto qos trust**, or **auto qos classify** command on an interface. Global and interface configurations on the switch migrate to the enhanced video or trust auto-QoS configurations.

  Explicit migration to enhanced auto-QoS occurs on a switch when you enable the **auto qos srnd4** global configuration command. You can configure the [**no**] form of this commandafter you remove auto-QoS functionality from all switch interfaces.

Documentation Updates

Update to the Device Manager Online Help

For Catalyst Switch Module 3110G and 3012, the physical LED behavior is different from the LED behavior on the device manager.

Updates to the Switch Getting Started Guide

When you launch Express Setup, you are prompted for the switch password. Enter the default password, *cisco*. The switch ignores text in the username field. Before you complete and exit Express Setup, you must change the password from the default password, *cisco*.

Update to the Switch Hardware Installation Guide

Catalyst Switch Module 3110X running Cisco IOS Release 12.2(52)SE or later ships with the Cisco TwinGig Converter Module (model CVR-X2-SFP) installed.

Updates to the System Message Guide

New System Messages

Error Message `AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface [chars], new MAC address ([enet) is seen. AuditSessionID [chars]`

Explanation A host on the interface attempted to gain access to the network or attempted an authentication. The interface mode does not support the number of hosts that are attached to the interface. This is a security violation, and the interface has been error-disabled. The first [chars] is the interface, [enet] is the Ethernet address of the host, and the second [chars] is the session ID.

Recommended Action Make sure that the interface is configured to support the number of hosts that are attached to it. Enter the **shutdown** interface configuration command followed by **no shutdown** interface configuration command to restart the interface.

Error Message `AUTHMGR-5-VLANASSIGN: VLAN [dec] assigned to Interface [chars] AuditSessionID [chars]`

Explanation A VLAN was assigned. [dec] is the VLAN ID, the first [chars] is the interface, and the second [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-FAILOVER: Failing over from [chars] for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation The authorization manager is failing over from the current authentication method to another method. The first [chars] is the current authentication method, the second [chars] is the client ID, the third [chars] is the interface, and the fourth [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 for the client, but authentication has failed. 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. If local authorization has been configured, the port will be authorized based on the local authorization method. Otherwise, authentication will restart according to the configured reauthentication period.

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-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 `HARDWARE-3-PORTNUM_ERROR: [traceback] port number [dec] is invalid`

Explanation The port number is out of range. [dec] is the port number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `HULC_LICENSE-1-LICENSE_REGISTER_FAILED: [chars] - rc = [dec]`

Explanation The licensing initialization failed. [chars] explains what part of the license registration failed, and [dec] is the type of license initialization error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `IFMGR-3-IFINDEX_PERSIST_ENTRY_CORRUPT: [chars] seems to be corrupted. Trying to read [dec] size`

Explanation The ifIndex table is corrupted. [chars] is the path to the IfIndex file, and [dec] is the number of bytes that was being read from the ifIndex table when the corruption was detected.

Recommended Action Delete the ifindex table.

Error Message `IFMGR-3-INVALID_PERSISTENT_DATA: Invalid persistent data`

Explanation The interface manager attempts to write invalid persistent data.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Error Message `SCHED-3-UNEXPECTEDEVENT: [traceback] [process information] Process received unknown event (maj [hex], min [hex])`

Explanation A process did not handle an event. The first [hex] is the major event number, and the second [hex] is the minor event number, both of which allow you to identify the event that occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Modified System Messages

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

Explanation 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.

Recommended Action No action is required.

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 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.

Note This message applies to switches running the IP base image.

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 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 port mode so that it is no longer a PVLAN host port, or use a valid secondary VLAN.

Note This message applies to switches running the IP base image.

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

Note This message applies to switches running the IP base image.

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 port mode 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 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_MDA_INACTIVE: Multi-Domain Authentication cannot activate because Data and Voice VLANs are the same on port AuditSessionID [chars]`

Explanation Multi-Domain Authentication (MDA) host mode cannot start when the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port session ID.

Recommended Action Change either the voice VLAN or the access VLAN on the interface so that they are not the same. MDA then starts.

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 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 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 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.

Recommended Action 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 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 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 shut down, or use another VLAN.

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

Explanation An attempt was made to assign a VLAN to a supplicant on a routed port, which is not allowed. [dec] is the VLAN ID, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Either disable the VLAN assignment, or change the port type to a nonrouted port.

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

Explanation An attempt was made to assign a VLAN to a promiscuous 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 Change the port mode so that it is no longer a promiscuous port, or change the configuration so that no VLAN is assigned.

Error Message `DOT1X_SWITCH-5-ERR_VLAN_RESERVED: Attempt to assign reserved 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 a reserved VLAN and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the seconds [chars] is the session ID.

Recommended Action Assign a different VLAN.

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 AuditSessionID [chars]`

Explanation Remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Either disable remote SPAN configuration on the VLAN, or disable IEEE 802.1x on all the ports in this VLAN.

Error Message `SPANTREE-2-BLOCK_BPDUGUARD_VP: Received BPDU on port [chars], vlan [dec] with BPDU Guard enabled. Disabling vlan.`

Explanation A BPDU was received on the interface and the VLAN specified in the error message. The spanning tree BPDU guard feature was enabled and configured to shut down the VLAN. As a result, the VLAN was placed in the error-disabled state. [chars] is the interface, and [dec] is the VLAN.

Recommended Action Either remove the device sending BPDUs, or disable the BPDU guard feature. The BPDU guard feature can be locally configured on the interface or globally configured on all ports that have Port Fast enabled. Re-enable the interface and vlan by entering the **clear errdisable** privileged EXEC command.

Deleted System Messages

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

Explanation The system memory is not sufficient to perform the IEEE 802.1x authentication.

Recommended Action Reduce other system activity to reduce memory demands.

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

Explanation Authentication was successful. [chars] is the interface.

Recommended Action No action is required.

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [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, and [chars] is the interface.

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

Explanation This message means that the VTP code encountered an unusual diagnostic situation. [chars] is a description of the situation.

Recommended Action Find out more about the error by using the s**how tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to

look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information.

Related Documentation

For more information about the switch module, see these documents on Cisco.com:

http://www.cisco.com/en/US/products/ps8741/tsd_products_support_series_home.html

- *Cisco Catalyst Switch Module 3110 and 3012 for IBM BladeCenter Software Configuration Guide*
- *Cisco Catalyst Switch Module 3110 and 3012 for IBM BladeCenter Command Reference*
- *Cisco Catalyst Switch Module 3110 and 3012 for IBM BladeCenter System Message Guide*
- *Cisco Software Activation Document for IBM*
- *Cisco Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter Hardware Installation Guide*
- *Cisco Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter*

For more information about the IBM BladeCenter enclosure, see the IBM documentation at:

http://www-03.ibm.com/systems/bladecenter/

These 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

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*
- *Network Admission Control Software Configuration Guide*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

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