



Release Notes for Cisco Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter, Cisco IOS Release 12.2(52)SE

Revised November 2, 2009

Cisco IOS Release 12.2(52)SE runs only on Catalyst Switch Module 3110G, 3110X, and 3012.

These release notes include important information about Cisco IOS Release 12.2(52)SE and later 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://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches>

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

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

For the complete list of Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter documentation, see the “[Related Documentation](#)” section on page 32.



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

Contents

- “System Requirements” section on page 2
- “Upgrading the Switch Module Software” section on page 4
- “Installation Notes” section on page 7
- “New Features” section on page 7
- “Minimum Cisco IOS Release for Major Features” section on page 8
- “Limitations and Restrictions” section on page 11
- “Important Notes” section on page 17
- “Open Caveats” section on page 19
- “Resolved Caveats” section on page 20
- “Documentation Updates” section on page 23
- “Related Documentation” section on page 32
- “Obtaining Documentation, Obtaining Support, and Security Guidelines” section on page 33

System Requirements

- “Hardware Supported” section on page 2
- “Device Manager System Requirements” section on page 3
- “CNA Compatibility” section on page 4

Hardware Supported

Table 1 lists the hardware supported on this release.

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 Switches running Cisco IOS Release 12.2(52)SE or later ship with the Cisco TwinGig Converter Module (model CVR-X2-SFP) installed.	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

Table 1 Catalyst Switch Module Supported Hardware (continued)

Switch Module Hardware	Description	Supported by Minimum Cisco IOS Release
Cisco X2 transceiver modules	X2-10GB-SR V02 or later X2-10GB-CX4 V03 or later X2-10GB-LX4 V03 or later 10 Gigabit Ethernet X2 ZR optical modules	Cisco IOS Release 12.2(40)EX2 Cisco IOS Release 12.2(50)SE
SFP modules	SFP-10G-SR SFP-10G-LR	Cisco IOS Release 12.2(50)SE

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 (BC-HT)	Yes	Yes	Yes
BladeCenter S (BC-S)	No	No	Yes
BladeCenter Multi-switch Interconnect Module (MSIM)	Yes ¹	Yes ¹	Yes

1. The advanced Management Module (aMM) firmware must use Version 1.42i or higher.

Device Manager System Requirements

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

- [“Hardware Requirements” section on page 3](#)
- [“Software Requirements” section on page 4](#)

Hardware Requirements

Table 3 lists the minimum hardware requirements for running the device manager.

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 lists the filenames for this software release.

Table 4 Cisco IOS Software Image Files for Catalyst Switch Modules

Filename	Description
cbs31x0-universal-tar.122-52.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.122-52.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.

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/12_2/configfun/command/reference/ffun_r.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. If you have a SmartNet support contract, go to this URL, and log in to download the appropriate files:

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

To download the universal software image files for a switch module, click **Cisco Catalyst Blade Switch 3000 Series for IBM**.

- 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.122-40.EX.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 Features

These sections describe the new supported hardware and the new and updated software features provided in this release:

- [“New Hardware Features” section on page 7](#)
- [“New Software Features” section on page 7](#)

New Hardware Features

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

New Software Features

- Full QoS support for IPv6 traffic.
- Smart Install to allow a single point of management (director) in a network. You can use Smart Install to provide zero touch image and configuration upgrade of newly deployed switches and image and configuration downloads for any client switches.
- Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports.
- Support for IP source guard on static hosts.

- RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.
- IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.
- Customizable web authentication enhancement to allow the creation of user-defined *login*, *success*, *failure* and *expire* web pages for local web authentication.
- Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.
- VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.
- MAC move to allow hosts (including the hosts connected behind 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 in the same way as a completely new MAC address.
- Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.
- 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.
- Support for VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port.
- Support for the LLPD-MED MIB and the CISCO-ADMISSION-POLICY-MIB.
- Support for up to 32 10 Gigabit Ethernet DWDM X2 optical modules.

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
Full QoS support for IPv6 traffic.	12.2(52)SE	3110G, 3110X, and 3012
Smart Install to allow a single point of management (director) in a network. You can use Smart Install to provide zero touch image and configuration upgrade of newly deployed switches and image and configuration downloads for any client switches.	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
Cisco Medianet to enable intelligent services in the network infrastructure for a wide variety of video applications. One of the services of Medianet is auto provisioning for Cisco Digital Media Players and Cisco IP Video Surveillance cameras through Auto Smartports.	12.2(52)SE	3110G, 3110X, and 3012
Support for IP source guard on static hosts.	12.2(52)SE	3110G, 3110X, and 3012
RADIUS Change of Authorization (CoA) to change the attributes of a certain session after it is authenticated. When there is a change in policy for a user or user group in AAA, administrators can send the RADIUS CoA packets from the AAA server, such as Cisco Secure ACS to reinitialize authentication, and apply to the new policies.	12.2(52)SE	3110G, 3110X, and 3012
IEEE 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.	12.2(52)SE	3110G, 3110X, and 3012
Support for critical VLAN with multiple-host authentication so that when a port is configured for multi-auth, and an AAA server becomes unreachable, the port is placed in a critical VLAN in order to still permit access to critical resources.	12.2(52)SE	3110G, 3110X, and 3012
Customizable web authentication enhancement to allow the creation of user-defined <i>login</i> , <i>success</i> , <i>failure</i> and <i>expire</i> web pages for local web authentication.	12.2(52)SE	3110G, 3110X, and 3012
Support for Network Edge Access Topology (NEAT) to change the port host mode and to apply a standard port configuration on the authenticator switch port.	12.2(52)SE	3110G, 3110X, and 3012
VLAN-ID based MAC authentication to use the combined VLAN and MAC address information for user authentication to prevent network access from unauthorized VLANs.	12.2(52)SE	3110G, 3110X, and 3012
MAC move to allow hosts (including the hosts connected behind 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 in the same way as a completely new MAC address.	12.2(52)SE	3110G, 3110X, and 3012
Support for including a hostname in the option 12 field of DHCPDISCOVER packets. This provides identical configuration files to be sent by using the DHCP protocol.	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

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 VTP version 3 that includes support for configuring extended range VLANs (VLANs 1006 to 4094) in any VTP mode, enhanced authentication (hidden or secret passwords), propagation of other databases in addition to VTP, VTP primary and secondary servers, and the option to turn VTP on or off by port.	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 and 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, also referred to as enhanced PAGP	12.2(46)SE	3110G, 3110X, and 3012
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 for the preassignment of an IP address to a switch port	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

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
IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router.	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.

This section contains these limitations:

- [“Cisco IOS Limitations” section on page 11](#)
- [“Device Manager Limitations” section on page 16](#)
- [“IBM BladeCenter Advanced Management Module Limitations” section on page 16](#)

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 12](#)
- [“Cisco X2 Transceiver Modules” section on page 12](#)
- [“Configuration” section on page 12](#)
- [“IEEE 802.1x Authentication” section on page 13](#)
- [“Multicasting” section on page 14](#)
- [“QoS” section on page 15](#)
- [“RADIUS” section on page 15](#)
- [“Routing” section on page 15](#)
- [“Stacking” section on page 16](#)
- [“SPAN and RSPAN” section on page 16](#)

Access Control List

This is the access control list (ACL) limitation:

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

This is an Address Resolution Protocol limitation:

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

These are the Cisco X2 transceiver module limitations:

- 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. (CSCsg28558)
- 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

These are the configuration limitations:

- 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-channell
(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 incorrectly allows the configuration. Port security is not supported on Gigabit Ethernet interface n/0/14.

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)

IEEE 802.1x Authentication

These are the IEEE 802.1x authentication limitations:

- 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

These are the multicasting limitations:

- 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)

QoS

These are the quality of service (QoS) limitations:

- 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)

RADIUS

This is the RADIUS limitation:

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

There is no workaround. (CSCta05071)

Routing

This is the routing limitation:

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)

Stacking

This is the stacking limitation:

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)

SPAN and RSPAN

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

- 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)

- 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 (CSCsg91027):

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

Device Manager Limitations

This is the device manager limitation:

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

This is the advanced Management Module (aMM) limitation:

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.

Important Notes

These sections describe the important notes related to this software release for the Catalyst Switch Module 3110G, 3110X, and 3012:

- [“Cisco IOS Notes” section on page 17](#)
- [“Device Manager Notes” section on page 17](#)

Cisco IOS Notes

This note applies to Cisco IOS software:

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

These notes apply to the device manager:

- 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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {aaa enable local}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> • 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	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	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	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>ip http authentication {enable local tacacs}</code>	Configure the HTTP server interface for the type of authentication that you want to use. <ul style="list-style-type: none"> • 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	<code>end</code>	Return to privileged EXEC mode.
Step 4	<code>show running-config</code>	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

Unless otherwise noted, these Cisco IOS configuration caveats apply to the Catalyst Switch Module 3110G, 3110X, and 3012:

- CSCsy85676

When you configure an ACL and enter the **access-group** interface configuration command to apply it to an interface for web authentication, the output from the **show epm session ip-address** or **show ip access_list interface interface-id** privileged EXEC command does not show any web authentication filter ID.

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.

- CSCtb08823

SNMP requests on the stpxRSTPPortRoleTable object only return information for the stack master.

There is no workaround.

- CSCtb25230

When a switch stack is configured with DHCP snooping enabled on the host VLAN, hosts connected to the stack master receive bootp packets, but the a packet might not be forwarded to the end hosts connected to stack member switches. The behavior depends on which interface in the stack received the packet.

The workaround is to disable DHCP snooping for the affected VLAN.

- CSCtb88425

If you press the MODE button to enter Express Setup setup mode after the switch has received an IP address dynamically through DHCP, HTTP authentication with the default username and password *cisco/cisco* fails.

Use one of these workarounds:

- Downgrade the image to 12.2(46)SE where there is no HTTP authentication.
- Use the console to perform initial configuration.

- 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.

Resolved Caveats

This release resolves these previously open caveats:

- CSCso35214

When you remove a switch module from a switch stack, the switch module Fa0 management interface remains administratively down and cannot be enabled by using the CLI.

The workaround is to reload the switch module.
- CSCso43123

(Only Catalyst Switch Module 3110X) When you move a blade server installed in slot 14 to another blade enclosure slot and install a new server in slot 14, unicast traffic from the original server to the new server might not be forwarded.

No workaround is needed. The problem corrects itself when the dynamic MAC address learning period times out. The default timeout is 5 minutes and is configurable in the CLI.
- CSCsw68528

On switches running Cisco IOS Release 12.2(44)SE or 12.2(46)SE, when you enter the **show mvr interface interface-id members** privileged EXEC command to see status of an MVR port, an MVR member port that is not connected always shows as *ACTIVE*.

The workaround is to use the **show mvr interface interface-id** or the **show mvr members** privileged EXEC command. These command outputs show the correct status of an MVR port.
- CSCsw69015

When you enter the **mvr vlan vlan-id** global configuration command to create an MVR VLAN and enable MVR on the switch by entering the **mvr** global configuration command, if you enter the **show mvr interface interface-id members** privileged EXEC command, the output shows the MVR groups on the interface. However, if you enable MVR first and then create the MVR VLAN, the MVR groups are not displayed correctly.
- CSCsw69335

In a stacked environment, IP ACLs are not applied to interfaces on member switches unless IP routing is enabled.

The workaround when applying IP ACLs to stack member interfaces is to enable IP routing on the stack master by entering the **ip routing** global configuration command.
- CSCsw96933

A switch running Cisco IOS Release 12.2(46)SE might lose packets for up to 30 seconds when a link fails. This occurs in some multiple spanning-tree (MST) topologies.

There is no workaround.
- CSCsx34798

The management port (Fa0) is shut down when a Telnet session is opened on the port from the chassis GUI. This occurs when the switch is in a stack and the stack members are powered down by using the chassis GUI.

The workaround is to reload the switch.
- CSCsx44525

If a Advanced Management Module (AMM) acts as a fail-over backup to another AMM, the ARP tables are not populated correctly.

There is no workaround.

- CSCsx71632

When VLAN-based quality of service (QoS) is enabled and then disabled on an interface by entering the **mls qos vlan-based** interface configuration command followed by the **no** version of the command, the port policy is not applied properly and could result in undefined behavior for packets matching the port policy.

The workaround is to remove the port policy by entering the **no service-policy input policy-map-name** interface configuration command and then reapply it to the interface.

- CSCsx78068

If you enable 802.1Q native VLAN tagging by entering the **vlan dot1q tag native** global configuration command and then change the native VLAN ID on an ingress trunk port by entering the **switchport trunk native vlan vlan-id** interface command, untagged traffic is forwarded instead of being dropped.

The workaround is to use one of these methods:

- Enter a **shutdown** followed by a **no shutdown** interface configuration command on the trunk port.
- Disable and then reenables native VLAN tagging by entering the **no vlan dot1q tag native** global configuration command followed by the **vlan dot1q tag native** command.

- CSCsy90265

If you repeatedly enter the **show tech-support** privileged EXEC command, the switch might leak memory and, in some cases, shut down.

The workaround is to reload the switch to clear the memory after repeated use of the **show tech-support** command.

- CSCsz66428

When flow control is enabled on a port-channel interface and you enter the **flowcontrol receive on** interface configuration command, the bundle is not enabled after the switch restarts. The command appears in the port-channel interface running configuration but does not appear in the switch running configuration. A message such as this appears:

```
%EC-5-CANNOT_BUNDLE2: Gi0/27 is not compatible with Po1 and will be suspended (flow control receive of Gi0/27 is on, Po1 is off)
%EC-5-CANNOT_BUNDLE2: Gi0/28 is not compatible with Po1 and will be suspended (flow control receive of Gi0/28 is on, Po1 is off)
```

Use one of these workarounds:

- To manually configure the port-channel interface, enter the **flowcontrol receive on** interface configuration command.
- To add the flow-control configuration to the interface after the switch restarts, use an EEM script similar to this:

```
event manager applet Add_flowcontrol_on_restart
event syslog pattern SYS-5-RESTART
action 1 cli command "en"
action 2 cli command "conf t"
action 3 cli command "inter port 1"
action 4 cli command "flowcontrol receive on"
```

For *action 3*, specify the port-channel interface.

- CSCsz72234

In a VPN routing/forwarding (VRF) instance, a port channel is configured, and the default route is in the global routing table. If a link shuts down while the other links remain up, the port channel might not forward traffic.

Use one of these workarounds:

- Enter the **shutdown** interface configuration command, and then enter the **no shutdown** interface command.
- In the VRF instance, configure the links in the port channel as Layer 2 access links, and configure a switch virtual interface (SVI).

- CSCsz88857

When an interface on the stack master is a member of an EtherChannel and the channel group number is removed before a master switch changeover, you can not use the same group number when you recreate the EtherChannel after the changeover.

These are possible workarounds:

- Reload the switches in the EtherChannel into the channel group that you were not able to create.
- Use a new channel group number to bundle the physical interfaces in an EtherChannel.
- Reconfigure the EtherChannel before the master switch changeover.

- CSCsy89011

Communication between the blade switch and blade server breaks after upgrading the switch from 12.2(40)EX2 to 12.2(46)SE under these conditions:

- mac-address-table on the switch does not show the internal host MAC.
- When we ping the internal host IP from the switch console, the ping fails leaving temporary ARP entry for the IP with incomplete mac-address.

The workaround is to disable the native vlan tagging feature and then do 'shut' and 'no shut' on the interface.

- CSCta10012

The user saw the error message about port 20 as following:

```
027562: Jun 3 12:29:38.357 PDT: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on GigabitEthernet0/20 (1), with RCOBC01 GigabitEthernet0/20 (1002).
```

On the blade switch 3012 switch, we can only see 18 ports. Logged from the management console and port 20 can not be modified as well

The workaround is to reload the switch that shows native VLAN in the message

- CSCta53893

If the host is in multiple-authentication (multiauth) mode and you configure the fallback authentication process as IEEE 802.1x or MAC authentication bypass, the per-user ACL does not work when the port uses web authentication as the fallback method and then uses 802.1x or MAC authentication bypass as the fallback method.

The workaround is to restart the switch.

- CSCta57846

The switch unexpectedly reloads when copying a configuration file from a remote server or from flash memory containing logging file flash:

The workaround is to enter the **logging file flash:filename** global configuration command to configure logging to flash instead of copying to flash.

- CSCta61664

Speed auto negotiation is turned “off” on the other side.

Workaround: Speed auto negotiation is turned “on” on the other side.

- CSCta78502

When you have configured a login banner by entering the **banner login c message c** global configuration command and the switch reloads, the output of banner is missing a carriage return, making the format incorrect.

There is no workaround.

- CSCta80514

When you enable MAC address learning on a VLAN and then change the interface configuration (such as adding the VLAN to the list of VLANs allowed on a trunk), MAC address learning is not disabled on the interface. If you disable MAC address learning on the switch, high CPU utilization occurs when the local forwarding manager tries to ut does not learn MAC addresses.

There is no workaround.

- CSCtb54305

You cannot configure private VLANs on port 14 on the Cisco Catalyst Switch Module 3110X.

There is no workaround.

- CSCtb77378

When you use IEEE 802.1x authentication with web authentication and an HTTP page opens, the switch redirects the user to an HTTP login page, not a HTTPS login page.

The workaround is to remove the custom banner.

- CSCtb84303

In a switch stack, when the SNMP vlan change (vmMembershipEntry) MIB is sent to a member switch other than the stack master, line protocol and notification flapping occurs.

There is no workaround.

- CSCtb97439

When remote neighbors change, the LLDP MIB does not properly update the remote neighbors.

The workaround is to clear the LLDP table by entering the **clear lldp table** privileged EXEC command.

Documentation Updates

- [Updates to the Software Documentation, page 24](#)
- [Update to the Device Manager Online Help, page 25](#)
- [Updates to the Switch Getting Started Guide, page 25](#)
- [Updates to the System Message Guide, page 26](#)

Updates to the Software Documentation

- The switch does not support ISL trunking.

Update to the “Configuring IEEE 802.1x Port-Based Authentication” Chapter

Common Session ID

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

The session ID includes:

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

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

```
Switch# show authentication sessions
```

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

This is an example of how the session ID appears in the syslog output. The session ID in this example is also 160000050000000B288508E5:

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

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

Update to the “Configuring Embedded Event Manager” Chapter

Embedded Event Manager 3.2

Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS device. EEM offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs.

EEM 3.2 is supported in Cisco IOS Release 12.2(52)SE and later releases, and introduced many new features.

EEM 3.2 introduces the following new event detectors:

- Neighbor Discovery—Neighbor Discovery event detector provides the ability to publish a policy to respond to automatic neighbor detection when:
 - a Cisco Discovery Protocol (CDP) cache entry is added, deleted, or updated.
 - a Link Layer Discovery Protocol (LLDP) cache entry is added, deleted, or updated.
 - an interface link status changes.
 - an interface line status changes.
- Identity—Identity event detector generates an event when AAA authorization and authentication is successful, when failure occurs, or after normal user traffic on the port is allowed to flow.
- Mac-Address-Table—Mac-Address-Table event detector generates an event when a MAC address is learned in the MAC address table.



Note The Mac-Address-Table event detector is supported only on switch platforms and can be used only on Layer 2 interfaces where MAC addresses are learned. Layer 3 interfaces do not learn addresses and routers do not usually support the mac-address-table infrastructure needed to notify EEM of a learned MAC address.

EEM 3.2 also introduces new CLI commands to support the applets to work with the new event detectors. For further details about EEM 3.2 features, see the Embedded Event Manager 3.2 document.

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_3.2.html

For the complete EEM document set, see these documents:

- *Embedded Event Manager Overview*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html
- *Writing Embedded Event Manager Policies Using the Cisco IOS CLI*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_cli.html
- *Writing Embedded Event Manager Policies Using Tcl*
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html

Update to the Device Manager Online Help

This is the update to switch module 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

These messages were added:

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-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-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]

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

Recommended Action No action is required.

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

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

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

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

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

Recommended Action Use a different VLAN.

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

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

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

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

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

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

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

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

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

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

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

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

Error Message DOT1X_SWITCH-5-ERR_VLAN_EQ_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 if 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 IEEE 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

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

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

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

Explanation Assign a different VLAN.

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

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

Recommended Action Update the configuration to use a valid VLAN.

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

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

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

These messages have been deleted:

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

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

Recommended Action Use a different VLAN.

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

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

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

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

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

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

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

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, and [chars] is the port.

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

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

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

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 [chars]

Recommended Action Multi-Domain Authentication (MDA) host mode cannot start if the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port.

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.

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

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

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

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

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]

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

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 [dec] to 802.1x port [chars]

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

Recommended Action Make sure that the VLAN exists and is not shut down, or use another VLAN.

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

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]

Explanation An attempt was made to assign a VLAN to a promiscuous IEEE 802.1x port, which is not allowed. [dec] is the VLAN, and [chars] is the port.

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]

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, and [chars] is the port.

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

Explanation This message means that remote SPAN should not be enabled on a VLAN with IEEE 802.1x-enabled. [dec] is the VLAN, and [chars] is the port.

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

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc. All rights reserved.

