Release Notes for Cisco Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter, Cisco IOS Release 15.0(2)SE and Later

April 16, 2014

These release notes include important information about Cisco IOS Release 15.1(2)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 this site (registered Cisco.com users with a login password):

http://www.cisco.com/cisco/software/navigator.html

For the complete list of Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter documentation, see the "Related Documentation" section on page 27.

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 Only version 02 or later CX1[2] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	12.2(55)SE1

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

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

The device manager verifies the browser version when starting a session and 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/cna_doc

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-universalk9-tar.150-2.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/software/navigator.html

b. Navigate to your switch model.

c. 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

New in Cisco IOS Release 15.0(2)SE1

- Support for Right-To-Use (RTU) licensing, which allows you to upgrade from one license level to another by entering commands in the command line interface without interacting with the Cisco Product License Registration portal.

New in Cisco IOS Release 15.0(2)SE

- Support for IPv6 multicast routing. For more information, see the *Implementing IPv6 Multicast* chapter of the software configuration guide on Cisco.com.

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
IPv6 multicast routing	15.0.2(SE)	3110G and 3110X
Protocol storm protection	12.2(58)SE1	3110G, 3110X, and 3012
VACL logging	12.2(58)SE1	3110G, 3110X, and 3012
Memory consistency check routine enhancements	12.2(58)SE1	3110G, 3110X, and 3012
Smart Call Home	12.2(58)SE1	3110G, 3110X, and 3012
IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates	12.2(58)SE1	3110G, 3110X, and 3012
Network Time Protocol version 4 (NTPv4)	12.2(58)SE1	3110G, 3110X, and 3012
DHCPv6 bulk-lease query	12.2(58)SE1	3110G, 3110X, and 3012
DHCPv6 relay source configuration	12.2(58)SE1	3110G, 3110X, and 3012
Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.	12.2(58)SE1	3110G, 3110X, and 3012
NSF IETF mode for OSPFv2	12.2(58)SE1	3110G, 3110X, and 3012
NSF IETF mode for OSPFv3	12.2(58)SE1	3110G, 3110X, and 3012
Virtual Router Redundancy Protocol (VRRPv4)	12.2(58)SE1	3110G, 3110X, and 3012
Support for deny ACL entries in Web Cache Communication Protocol (WCCP) redirect lists	12.2(58)SE1	3110G, 3110X, and 3012
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
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

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 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
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

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).	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

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

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))

Bootloader

- 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. (CSCta72141)

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)

- 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. (CSCtf34659)

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)

VLANs

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

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

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

- CSCtg98453

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

  There is no workaround.

- CSCtl60247

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

  There is no workaround.

Resolved Caveats

Caveats Resolved in Cisco Release 15.0(2)SE6

- CSCue95644

  When you upgrade a device to a Cisco IOS or Cisco IOS XE release that supports Type 4 passwords, enable secret passwords are stored using a Type 4 hash which can be more easily compromised than a Type 5 password.

  The workaround is to configure the **enable secret** command on an IOS device without Type 4 support,copy the resulting Type 5 password, and paste it into the appropriate command on the upgraded IOS device.

- CSCuh51379

  When VTp mode is set to transparent and vlan.dat file present in flash is deleted, after reload, access vlan is not configured in the switch even though vlan configuration is present in running config or startup config does not get copied to the startup configuration file.

  There is no workaround.

- CSCui96653

  On a switch stack, when you perform a master switch over and run the **show run** command on the new master switch, the switch displays the following error message and associated traceback.

  ```
  %SYS-2-CCA_INT_ERR: CCA Detected Logic Error, code = 12
  ```

  There is no workaround.

- CSCto13462

  In a network that consists of two DHCP clients with same client id and different mac addresses, the DHCP server reloads when one of the clients releases its DHCP address.

  The workaround is to set the vtp mode to server or client.

- CSCts80209

  A switch configured with login quiet-mode resets when you enter the **login block-for** or **no login block-for** commands.

  There is no workaround. To avoid a reset, do not enter the **login block** or **no login block-for** command.

Caveats Resolved in Cisco IOS Release 15.0(2)SE5

- CSCua00661

  A memory leak is observed when configuring VLANs using tclsh mode.

  The workaround is to make the tclsh mode interactive to avoid any memory leak.

- CSCua17863 (Catalyst Blade Switch 3032)

  After rebooting the switch, the Ethernet management port (Fa0) goes to half-duplex mode and might display the following CDP warning message.

  ```
  DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0 (not full duplex)
  ```

  The **show interface** command output indicates that the interface goes to half-duplex mode but there is no late collision counter or packet impact observed.

  The workaround is to use the **no cdp run** command on the switch.

- CSCue94252

  When the **privilege exec level 5 show mac address-table interface gigabitethernet** privileged EXEC command is entered, all interfaces in the switch have the command applied to the running configuration.

  There is no workaround.

- CSCug26848

  CPU usage goes above 90% when Internet Group Management Protocol (IGMP) version 3 report packets are sent to the switch which has IGMP version 2 configured on the switch virtual interface.

  The workaround is to either disable multicast fast convergence or configure IGMP version 3 on switch virtual interface.

- CSCug51225

  Topology Change Notification (TCN) occurs over the network when a new stack member is added to the switch stack.

  There is no workaround

- CSCug52714

  TACACS+ single connect authentication request from a switch stack takes around 10 to 12 minutes to failover to secondary server after the primary TACACS server is unreachable.

  The workaround is to disable TACACS+ single connect configuration on the switch.

- CSCuh75095

  After rebooting a Cisco Catalyst Blade Switch 3012 (CBS3012), incorrect data is found in the vital product data (VPD) of the switch, which causes the switch to become unmanageable.

  There is no workaround.

- CSCui41032

  Switch runs out of memory within few seconds of configuring the command **privilege exec level <n> show spanning-tree active/detail**.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE4

- CSCuf77683

  Internal VLANs are displayed when the **show snmp mib ifmib ifindex** command is entered or the SNMP is queried for the ipMIB object.

  The workaround is to check if the displayed VLANs are internal and then to hide them.

- CSCug62154

  When the switch is started using TACACS+ configurations, the CPU utilization increases to 100% and the VTY device does not work.

  The workaround is to remove the TACACS+ configurations and restart the switch.

- CSCuh41077

  The ipAddrEntry value in the IP Address Table shows an interface index that is not exposed by the ifEntry Object ID.

  There is no workaround.

Caveats Resolved in Cisco IOS Release 15.0(2)SE3

- CSCta43825

  CPU usage is high when an SNMP Walk of the Address Resolution Protocol (ARP) table is performed.

  The workaround is to implement SNMP view using the following commands:

  snmp-server view cutdown iso included

  snmp-server view cutdown at excluded

  snmp-server view cutdown ip.22 excluded

  snmp-server community public view cutdown ro

  snmp-server community private view cutdown rw

- CSCts95370

  If an ACL is configured on a router VTY line for ingress traffic, the ACL is applied for egress traffic also. As a result, egress traffic to another router on an SSH connection is blocked.

  The workaround is to permit egress traffic to the specific destination router using the **permit tcp host** <*destination router IP address*> **eq 0 any** interface configuration command.

- CSCub85948

  Memory leak is seen in the switch when it sends CDP, LLDP or DHCP traffic and when the link flaps.

  The workaround is to apply protocol filters to the device sensor output by entering the following global configuration commands:

  no macro auto monitor

  device-sensor filter-spec dhcp exclude all

  device-sensor filter-spec lldp exclude all

device-sensor filter-spec cdp exclude all

If the memory leak continues in the "DHCPD Receive" process, disable the built-in DHCP server by entering the **no service dhcp** global configuration command.

- CSCub88590

  Block0 of VPD data gets corrupted or overwritten at byte location 0 or 2. This may cause incorrect readings or cause incorrect information to be sent from the switch to the Advanced Management Module (AMM). Hence, managing the switch from the AMM may show incorrect results. (Data traffic is uninterrupted and management from Telnet or direct Web access works correctly.

  There is no workaround.

- CSCuc40634

  STP loop occurs on Flexstack connected by parallel links when a link state is changed on Flexlink port.

  The workaround is to change the switch to root bridge.

- CSCud96215

  LSG Downlink port flaps when SFP+ is used as an uplink port. This issue also appears if SFP+ is configured in a flexlink configuration.

  There is no workaround. The configuration recovers automatically

- CSCud83248

  When native VLAN is configured on the trunk or when switchport trunk native vlan 99 is configured on the interface, spanning-tree instance is not created for native VLAN.

  The workaround is to keep VLAN1 as a native on the trunk. In Cisco IOS Release15.0(2) SE, **dot1.x** is enabled by default and causes authentication fail in the native VLAN. This results in **pm_vp_statemachine** not triggering any event to spanning tree. To disable **dot1x** internally, run the **no macro auto monitor** command. The stp instance is created for native vlan 99 after running the **show** and **no show** command on the interface.

- CSCue83689

  In Catalyst stacked switches, when a member switch with VLAN assigned through Access Control Server (ACS) is configured for 802.1x authentication, the switch fails with the following messages:

  ```
  %SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "hpm main process", ipl=
  0, pid= 121
  OR
  %SYS-2-NOBLOCK: may_suspend with blocking disabled. -Process= "HRPC pm request
  handler", ipl= 0, pid= 130
  ```

  There is no workaround.

- CSCue87815

  When the secret password is configured, the password is not saved. The default password is used as the secret password.

  The workaround is to use the default password to login and then change the password.

- CSCug67158

  When booting up CBS3110 or CBS3012 switch with Cisco IOS Release 15.0(2)SE1 or 15.0(2)SE2, traceback messages about VPD MAC Address are displayed

  There is no workaround and there is no functional impact.

Caveats Resolved in Cisco IOS Release 15.0(2)SE1

- CSCee32792

  When using SNMP v3, the switch unexpectedly reloads when it encounters the snmp_free_variable_element.

  There is no workaround.

- CSCth03648

  When two traps are generated by two separate processes, the switch fails if one process is suspended while the other process updates variables used by the first process.

  The workaround is to disable all SNMP traps.

- CSCth59458

  If a redundant power supply (RSP) switchover occurs during a bulk configuration synchronization, some of the line configurations might disappear.

  The workaround is to reapply the line configurations.

- CSCtl12389

  The **show ip dhcp pool** command displays a large number of leased addresses.

  The workaround is to turn off **ip dhcp remember** and reload the switch.

- CSCtq64716

  The following warning messages might be displayed during the boot process even when a RADIUS or a TACACS server have been defined:

  ```
  %RADIUS-4-NOSERVNAME:
  ```

  or

  ```
  %AAAA-4-NOSERVER: Warning: Server TACACS2 is not defined
  ```

  There is no workaround.

- CSCtr37757

  The secure copy feature (**copy:** *source-filename* **scp**: *destination-filename* command) does not work.

  There is no workaround.

- CSCtz98066

  When the master switch (Switch A) is reloaded or loses power and rejoins the stack as a member switch, any traffic stream that exits Switch A is dropped because the newly joined member is not able to establish an Address Resolution Protocol (ARP) entry for the next hop router or switch. Debugs confirm that Switch A does not send a GARP or ARP for the next hop, though traffic continues to be sent to the switch.

  The workaround is to add a static ARP. Ping the destination from Switch A to force the ARP to respond.

- CSCub88590

  Data at Block 0 of the Cisco Vital Product Data (VPD) is corrupted or over-written at byte location 0 or 2. This may cause incorrect information to be sent from the switch to the Advanced Management Module (AMM).

  There is no workaround.

- CSCub93357

If an interface is configured with the **switchport port-security maximum 1 vlan** command, the following error message is displayed:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address XXXX.XXXX.XXXX on port <interface>
```

There is no workaround.

- CSCuc03555

  The flash memory is corrupted when you format the flash manually.

  The workaround is to reload the switch. (Note that this will erase the flash memory, and you will need to reload the software image using TFTP, a USB drive, or a serial cable.

- CSCuc17720

  If the Performance Monitor cache is displayed (using the **show performance monitor cache** command) and you attempt to stop the command output display by entering the **q** keyword, there is an unusually long delay before the output is stopped.

  The workaround is to enter the **term len 0** privileged EXEC command so that all command outputs are displayed without any breaks.

Caveats Resolved in Cisco IOS Release 15.0(2)SE

- CSCto78529

  After upgrading to Cisco IOS Release 12.2(58)SE1, the Fa0 port on the switch does not respond to the **ping** command.

  The workaround is to use Cisco IOS Release 12.2(55)SE.

- CSCtq51049

  In a switch stack, you cannot establish a console session with a member switch when an ACL is applied to the VTY lines.

  The workaround is to use the following procedure when you apply an ACL to line vty 0 4 and line vty 5 15:

  1. Create the **vty** ACL and permit the 127 network.
  2. Append the **vrf-also** keyword to the configured access-class inbound.

  See the following example:

```
ip access-list standard vty-acl
   permit 127.0.0.0 0.0.0.255

line vty 0 4
   access-class vty-acl in vrf-also
   privilege level 15
   length 0
   transport input ssh
line vty 5 15
   access-class vty-acl in vrf-also
   privilege level 15
   transport input ssh
```

- CSCtr07908

  The archive download feature does not work if the flash contains an “update” directory. This situation is likely to occur if a previous download failed or was interrupted and the “update”” directory is still left in the flash.

- CSCtr44361

  When a device is moved from one port to another in a switch stack, the SNMP data generated for the move event is incorrect.

  The workaround is to ensure that the uplink to the core network is configured on the master switch (for example, a 1/0/x port).

- CSCtr55645

  OSPFv3 neighbors might flap because of the way the switch handles IPv6 traffic destined for well-known IPv6 multicast addresses.

  There is no workaround.

- CSCts36715

  Users connecting to the network through a device configured for web proxy authentication may experience a web authentication failure.

  There is no workaround. Use the **clear tcp tcb** command to release the HTTP Proxy Server process.

- CSCtt11621

  Using the **dot1x default** command on a port disables access control on the port and resets the values of the **authentication host-mode** and **authentication timer reauthenticate** commands to the default values.

  The workaround is to avoid using the **dot1x default** command and set various dot1x parameters individually. You can also reconfigure the parameters that were changed after you entered the **dot1x default** command.

- CSCtx33436

  When using the **switchport port-security maximum** 1 **vlan access** command, if an IP-phone with a personal computer connected to it is connected to an access port with port security, a security violation will occur on the interface. This type of message is displayed on the console:

  ```
  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address
  XXXX.XXXX.XXXX on port FastEthernet0/1.
  ```

  Here is a sample configuration:

  ```
  interface gigabitethernet 3/0/47
  switchport access vlan 2
  switchport mode access
  switchport voice vlan 3
  switchport port-security maximum 2
  switchport port-security maximum 1 vlan access
  switchport port-security maximum 1 vlan voice
  switchport port-security
  ```

  The workaround is to remove the line **switchport port-security maximum** 1 **vlan access**.

- CSCtx96491

  The switch does not correctly detect a loopback when the switch port on an authenticated IP phone is looped to a port configured and authenticated with dot1x security, even when **bpduguard** is configured on the interface. This situation can result in 100 percent CPU utilization and degraded switch performance.

  The workaround is to configure the interface with the **authentication open** command or to configure **authentication mac-move permit** on the switch.

- CSCue23882

If a new port is added to an etherchannel on a switch using DAI or IPDT, ARP packets that ingress the port are lost.

The workaround is to save the configuration and reload the switch. Alternatively, configure the switch by entering the **no macro auto monitor** command followed by the **macro auto monitor** command after the port is bundled for the first time.

Related Documentation

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

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:
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:
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.