Release Notes for Cisco Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter, Cisco IOS Release 12.2(53)SE and Later

Revised March 24, 2010

Cisco IOS Release 12.2(53)SE and later runs only on Catalyst Switch Module 3110G, 3110X, and 3012.

These release notes include important information about Cisco IOS Release 12.2(53)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** "Finding the Software Version and Feature Set" section on page 5.

  If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 5.

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

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

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

For the complete list of Catalyst Switch Module 3110G, 3110X, and 3012 for IBM BladeCenter documentation, see the "Related Documentation" section on page 32.

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

Contents

System Requirements

Hardware Supported

Table 1 Catalyst Switch Module Supported Hardware

Switch Module Hardware	Description	Supported by Minimum Cisco IOS Release
	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**	

Catalyst Switch Module Supported Hardware (continued)

	Note	12.2(46)SE
SFP modules[1]	GLC-T GLC-SX-MM GLC-LH-SM SFP Modules require the use of TwinGig adapter (CVR-X2-SFP).	12.2(52)SE
Supports OneX (CVR-X2-SFP10G) and these SFP+ modules (For the Catalyst Switch Modules 3110G and 3110X)	SFP-10G-SR SFP-10G-LR SFP-10G-LRM Only version 02 or later CX1[2] cables are supported: SFP-H10GB-CU1M SFP-H10GB-CU3M SFP-H10GB-CU5M	12.2(53)SE

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

Table 2 IBM BladeCenter Supported Switch Modules

	Switch Module 3110G	**Switch Module 3110X**	**Switch Module 3012**
	Yes	Yes	Yes
BladeCenter S (BC-S)	No	No	Yes
BladeCenter Multi-switch Interconnect Module (MSIM)	Yes[2]	Yes[2]	Yes

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
	64 MB[2]	256	1024 x 768	Small

We recommend Intel Pentium 4.

2. We recommend 256-MB DRAM.

Software Requirements

-
-

CNA Compatibility

Release Notes for Cisco Network Assistant

Upgrading the Switch Module Software

-
-
-
-
-

Finding the Software Version and Feature Set

Note

filesystem:

Deciding Which Files to Use

download-sw **archive download**

Table 4 Cisco IOS Software Image Files for Catalyst Switch Modules

	This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.

Cisco Software Activation for IBM

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

Archiving Software Images

copy flash: tftp:

tftp-server

tftp-server

Cisco IOS Configuration Fundamentals Command Reference, Release 12.2,

Upgrading a Switch Module by Using the Device Manager or Network Assistant

Help

Upgrading a Switch Module by Using the CLI

Step 1

Step 2

Cisco Catalyst Switch Modules for IBM

Step 3

Step 4

Step 5

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

Step 6

archive download-sw /overwrite /reload
tftp:[[//*location*]/*directory* *image-name*.**tar**

/overwrite

/reload

//

/*image-name*.**tar**

tftp://198.30.20.19/cbs31x0-universal-tar.image-name.tar

Installation Notes

New Features

-
-

New Hardware Features

New Software Feature

ip vrf forwarding **ip radius source-interface**

Minimum Cisco IOS Release for Major Features

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

	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
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 , , and *expire*		

Feature	Minimum Cisco IOS Release Required	Catalyst Switch Module Support

Limitations and Restrictions

-
-
-
-

Cisco IOS Limitations

-
-
-
-
-
-
-
-

-
-
-

Access Control List

mac address-table static

vlan **drop**

Address Resolution Protocol

Cisco X2 Transceiver Modules

-
-
-

Configuration

-

```
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
```

```
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
```

```
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
```

{ | *stack-member-number*} privileged EXEC command, the complete output does not appear.

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

IEEE 802.1x Authentication

-
-
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -
  -

ip igmp max-groups **ip igmp max-groups action replace**

QoS

-
-
-
-
- **srr-queue bandwidth limit**

mls qos queue-set output *qset-id* *allocation1 ... allocation4*

RADIUS

Routing

Stacking

SPAN and RSPAN

-
-

Device Manager Limitations

Yes

IBM BladeCenter Advanced Management Module Limitations

SoL and cKVM

-
-
-
-

-
-
-
-
-

Important Notes

-
-

Cisco IOS Notes

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

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. **Tools > Internet Options**

   Settings

   Automatically

   OK

   OK

show running-config

configure terminal	
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 interface configuration command for the keyword to appear. —Enable password, which is the default method of HTTP server user authentication. —Local user database, as defined on the Cisco router or access server.
	Return to privileged EXEC mode.
	Verify your entries.

Location Address

configure terminal	
ip http authentication enable local tacacs	**enable** **local** **tacacs**
end	
show running-config	

cisco.com:84 *http://*

Open Caveats

- **ip access_list interface**

show interfaces

reload

write erase

vlan

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(53)SE1

-
-
-
-
-

snmp-server trap-source loopback0 **snmp-server source-interface informs loopback0**

-
-
-
-

no ip ftp passive

ip ftp passive

-
-

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(53)SE

-

no ntp

-

errdisable max flap 10 time 10 global

-

```
%SUPQ-4-CPUHB_RECV_STARVE: Still seeing receive queue stuck after throttling
```

```
%SUPQ-4-CPUHB_RECV_STARVE: Still seeing receive queue stuck after throttling
```

Documentation Updates

Updates to the Software Documentation

Update to the "Configuring IP Unicast Routing" Chapter

User Interface for VRF-Aware RADIUS

Per VRF AAA Feature Guide

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

Common Session ID

-
-
-

```
Fa4/0/4    0000.0000.0203  mab      DATA     Authz Success  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
```

Update to the “Configuring Embedded Event Manager” Chapter

Embedded Event Manager 3.2

-
-
-

Note

- *Embedded Event Manager Overview*
- *Writing Embedded Event Manager Policies Using the Cisco IOS CLI*

  Writing Embedded Event Manager Policies Using Tcl

	Path Cost Value

Update to the Device Manager Online Help

Updates to the Switch Getting Started Guide

Update to the Switch Hardware Installation Guide

Updates to the System Message Guide

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

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

Recommended Action

Error Message `OT1X-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]`

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

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

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

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

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

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]

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

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]

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]

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

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

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

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

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

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

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

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

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

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]

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

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

DOT1X_SWITCH-5-ERR_VLAN_EQ_MDA_INACTIVE: Multi-Domain Authentication cannot activate because Data and Voice VLANs are the same on port [chars]

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

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

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

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

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

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

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

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

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

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

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*

- *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

What's New in Cisco Product Documentation

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