Release Notes for Cisco Enhanced EtherSwitch Service Modules, Cisco IOS Release 15.0(2)EJ and Later

February 20, 2014

Cisco IOS Release 15.0(2)EJ and later runs on Cisco enhanced EtherSwitch service modules SM-X-ES3-16-P and SM-X-ES3-24-P. Cisco IOS Release 15.0(2)EJ1 runs on SM-X-ES3D-48-P.

Unless otherwise noted, the term *switch* refers to Cisco enhanced EtherSwitch service modules and supports the same features as that of Catalyst 3560-X switch. The terms *Cisco Catalyst 3560-X Switch* and *Cisco Enhanced EtherSwitch Service Modules* are used interchangeably in this document.

For more information, see the "Deciding Which Files to Use" section on page 4 and the "Related Documentation" section on page 21.

These release notes include important information about Cisco IOS Release15.0(2)EJ and higher, and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 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 4.

You can download the switch software from this site (registered Cisco.com users with a login password): http://www.cisco.com/cisco/web/download/index.html

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

Contents

System Requirements

Supported Hardware

Table 1 Enhanced EtherSwitch Service Modules

Service Module	Description	Supported by Minimum Cisco IOS Release
SM-X-ES3-16-P	EtherSwitch SM L3 + PoEPlus + MACSec + 16 10/100/1000	15.0(2)EJ
SM-X-ES3-24-P	EtherSwitch SM L3 + PoEPlus + MACSec + 24 10/100/1000	15.0(2)EJ
SM-X-ES3D-48-P	EtherSwitch SM L3 + PoEPlus + MACSec + 48 10/100/1000 + 2SFP	15.0(2)EJ1
SM-X-ES3-24-P-T	EtherSwitch SM L3 + PoEPlus + MACSec + 24 10/100/1000 (Temperature hardended)	15.2(2)E1

Device Manager System Requirements

Hardware

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software

- 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.

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3560-X switch, all standby command switches must be Catalyst 3560-X switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant*, *Release Notes for Cisco Network Assistant,* the Cisco enhanced EtherSwitch service module documentation, the software configuration guide, and the command reference.

CNA Compatibility

Cisco IOS 12.2(35)SE2 and later is only compatible with Cisco Network Assistant 5.0 and later. You can download Cisco Network Assistant from this URL:
http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

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

Upgrading the Switch Software

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. 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. The second line of the display shows the version.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and 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

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image and a specific software license. If you do not have a service support contract, such as a SMARTnet contract, download the IP base image from Cisco.com. The switches running the universal software images can use permanent and temporary software licenses. See the "Cisco IOS Software Activation Conceptual Overview" chapter in the *Cisco IOS Software Activation Configuration Guide*:
http://www.cisco.com/en/US/docs/ios/csa/configuration/guide/12.4T/csa_book.html

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.

Catalyst 3560-X switches running payload-encryption images can encrypt management and data traffic. Switches running nonpayload-encryption images can encrypt only management traffic, such as a Secure Shell (SSH) management session.

- Management traffic is encrypted when SSH, Secure Socket Layer (SSL), Simple Network Management Protocol (SNMP), and other cryptographic-capable applications or protocols are enabled.
- Data traffic is encrypted when MACsec is enabled.

For more information about Catalyst 3560-X software licenses and available images, see the *Cisco IOS Software Installation Document* on Cisco.com:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

Table 3 Software Images

Image	Filename	Description
Cisco Enhanced EtherSwitch Service Modules		
IP base without payload encryption	c3560e-ipbasek9npe-tar.150-2.EJ.tar	IP base image, as well as LAN base image with Layer 2 features

Table 3 Software Images (continued)

Image	Filename	Description
IP base with payload encryption	c3560e-ipbasek9-tar.150-2.EJ.tar	IP base image, as well as LAN base image with Layer 2 features
Universal without payload encryption	c3560e-universalk9npe-tar.150-2.EJ.tar	LAN base, IP base, and IP services software licenses
Universal with payload encryption	c3560e-universalk9-tar.150-2.EJ.tar	LAN base, IP base, and IP services software licenses
Universal with payload encryption	c3560e-universalk9-mz.tar	LAN base, IP base, and IP services software licenses

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 through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Archiving Software Images

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

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd80281c0e.html

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

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 as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*:
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.html

Upgrading a Switch by Using the Device Manager or Network Assistant

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

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

Upgrading a Switch by Using the CLI

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

To download software, follow these steps:

Step 1 Use Table 3 on page 4 to identify the file that you want to download.

Step 2 Download the software image file:

a. If you are a registered customer, go to this URL and log in: http://software.cisco.com/download/navigator.html?a=a&i=rpm

b. Navigate to **Switches > LAN Switches - Access**

c. Navigate to your switch model.

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

e. 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 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, see the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

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

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For **//***location*, specify the IP address of the TFTP server.

For */directory/image-name*.**tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/c3560e-universalk9npe-tar.150-2.EJ.tar
```

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

Recovering from a Software Failure

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

Installation Notes

Use these methods to assign IP information to your switch:

- The Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

Cisco IOS Limitations

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 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 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))

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 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 generates this notification when snooping the next ARP packet. (CSCse47548)
- When there is a VLAN with protected ports configured in 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 port configuration is set at 10 Mb/s 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)

- 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)

Diagnostics

- (Catalyst 3560-X switches) When you enter the **test cable-diagnostics tdr interface** or the **show cable-diagnostics tdr interface** privileged EXEC command on an interface to determine the length of a connected cable, the cable length might be reported as N/A. This can occur when there is no link, a 10 Mb/s link, or a 100 Mb/s link, even though there are no cable faults. Cable length is reported correctly when a 1 Gb/s link is active on the interface.

  The workaround to verify the cable length is to enter the commands when a Gigabit link is active on the interface or after disconnecting the far end of the cable. (CSCte43869)

EtherChannel

- In an EtherChannel running Link Aggregation Control Protocol (LACP), the ports might be put in the suspended or error-disabled state after a stack partitions or a member switch reloads. This occurs when:
  - The EtherChannel is a cross-stack EtherChannel with a switch stack at one or both ends.
  - The switch stack partitions because a member reloads. The EtherChannel is divided between the two partitioned stacks, each with a stack master.

  The EtherChannel ports are put in the suspended state because each partitioned stack sends LACP packets with different LACP Link Aggregation IDs (the system IDs are different). The ports that receive the packets detect the incompatibility and shut down some of the ports. Use one of these workarounds for ports in this error-disabled state:
  - Enable the switch to recover from the error-disabled state.
  - Enter the **shutdown** and the **no shutdown** interface configuration commands to enable the port.

  The EtherChannel ports are put in the error-disabled state because the switches in the partitioned stacks send STP BPDUs. The switch or stack at the other end of the EtherChannel receiving the multiple BPDUs with different source MAC addresses detects an EtherChannel misconfiguration.

  After the partitioned stacks merge, ports in the suspended state should automatically recover. (CSCse33842)
- When a switch stack is configured with a cross-stack EtherChannel, it might transmit duplicate packets across the EtherChannel when a physical port in the EtherChannel has a link-up or link-down event. This can occur for a few milliseconds while the switch stack adjusts the EtherChannel for the new set of active physical ports and can happen when the cross-stack EtherChannel is configured with either mode ON or LACP. This problem might not occur with all link-up or link-down events.

  No workaround is necessary. The problem corrects itself after the link-up or link-down event. (CSCse75508)

- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

```
15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
(ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
4CEB50 859DF4 A7BF28 A98260 882658 879A58
```

  There is no workaround. (CSCsh12472)

IEEE 802.1x Authentication

- 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 card 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.

- When IEEE 802.1x authentication with VLAN assignment is enabled, a CPUHOG message might appear if the switch is authenticating supplicants in a switch stack.

  The workaround is not use the VLAN assignment option. (CSCse22791)

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 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 the **clear ip mroute** privileged EXEC command is used 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 because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)

- When you configure the IGMP snooping throttle limit by using the **ip igmp max-groups** *number* interface configuration on a port-channel interface, the groups learned on the port-channel might exceed the configured throttle limit number, when all of these conditions are true:

  - The port-channel is configured with member ports across different switches in the stack.
  - When one of the member switches reloads.
  - The member switch that is reloading has a high rate of IP IGMP joins arriving on the port-channel member port.

  The workaround is to disable the IGMP snooping throttle limit by using the **no ip igmp max-groups** *number* interface configuration command and then to reconfigure the same limit again. (CSCse39909)

PoE or PoE+

- When a loopback cable is connected to a switch PoE port, the **show interface status** privileged EXEC command shows *not connected*, and the link remains down. When the same loopback cable is connected to a non-PoE port, the link becomes active and then transitions to the error-disabled state when the **keepalive** feature is enabled.

  There is no workaround. (CSCsd60647)

- The Cisco 7905 IP Phone is error-disabled when the phone is connected to an external power source.

  The workaround is to enable PoE and to configure the switch to recover from the PoE error-disabled state. (CSCsf32300)

- The pethPsePortShortCounter MIB object appears as *short* even though the powered device is powered on after it is connected to the PoE port.

  There is no workaround. (CSCsg20629)

- (Catalyst 3560-X switches) When a powered device (such as an IP phone) connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the switch locks to the power-negotiation protocol of that first packet. The switch does not respond to power requests from the other protocol. For example, if the switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch does not respond to LLDP power requests and can no longer power on any accessories.

  The workaround is to turn the powered device off and then on again.

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 rejects the configuration, and 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 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 is improved 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.

- 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

- The switch stack might reload if the switch runs with this configuration for several hours, depleting the switch memory and causing the switch to fail:

  - The switch has 400 Open Shortest Path First (OSPF) neighbors.
  - The switch has thousands of OSPF routes.

  The workaround is to reduce the number of OSPF neighbors to 200 or less. (CSCse65252)

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

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

Smart Install

- When upgrading switches in a stack, the director cannot send the correct image and configuration to the stack if all switches in the stack do not start at the same time. A switch in the stack could then receive an incorrect image or configuration.

  The workaround is to use an on-demand upgrade to upgrade switches in a stack by entering the **vstack download config** and **vstack download image** commands. (CSCta64962)

- When you upgrade a Smart Install director to Cisco IOS Release 12.2(55)SE but do not upgrade the director configuration, the director cannot upgrade client switches.

  When you upgrade the director to Cisco IOS Release 12.2(55)SE, the workaround is to also modify the configuration to include all built-in, custom, and default groups. You should also configure the tar image name instead of the image-list file name in the stored images. (CSCte07949)

- Backing up a Smart Install configuration could fail if the backup repository is a Windows server and the backup file already exists in the server.

  The workaround is to use the TFTP utility of another server instead of a Windows server or to manually delete the existing backup file before backing up again. (CSCte53737)

- In a Smart Install network with the backup feature enabled (the default), the director sends the backup configuration file to the client during zero-touch replacement. However, when the client is a switch in a stack, the client receives the seed file from the director instead of receiving the backup configuration file.

  The workaround, if you need to configure a switch in a stack with the backup configuration, is to use the **vstack download config** privileged EXEC command so that the director performs an on-demand upgrade on the client.

  - When the backup configuration is stored in a remote repository, enter the location of the repository.
  - When the backup file is stored in the director flash memory, you must manually set the permissions for the file before you enter the **vstack download config** command. (CSCtf18775)

- If the director in the Smart Install network is located between an access point and the DHCP server, the access point tries to use the Smart Install feature to upgrade even though access points are not supported devices. The upgrade fails because the director does not have an image and configuration file for the access point.

  There is no workaround. (CSCtg98656)

- When a Smart Install director is upgrading a client switch that is not Smart Install-capable (that is, not running Cisco IOS Release 12.2(52)SE or later), the director must enter the password configured on the client switch. If the client switch does not have a configured password, there are unexpected results depending on the software release running on the client:

  - When you select the NONE option in the director CLI, the upgrade should be allowed and is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.
  - When you enter any password in the director CLI, the upgrade should not be allowed, but it is successful on client switches running Cisco IOS Release 12.2(25)SE through 12.2(46)SE, but fails on clients running Cisco IOS Release 12.2(50)SE through 12.2(50)SEx.

There is no workaround. (CSCth35152)

SPAN and RSPAN

- When the RSPAN feature is configured on a switch, CDP packets received from the RSPAN source ports are tagged with the RSPAN VLAN ID and forwarded to trunk ports carrying the RSPAN VLAN. When this happens, a switch that is more than one hop away incorrectly lists the switch that is connected to the RSPAN source port as a CDP neighbor.

  This is a hardware limitation. The workaround is to disable CDP on all interfaces carrying the RSPAN VLAN on the device connected to the switch. (CSCeb32326)

- 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)

- (Catalyst 3560-X switches) When you enter the **show monitor** privileged EXEC command the monitor source port output is incorrect. This situation occurs only if the monitor source port(s) is a pluggable Gigabit module and you set any source port combination, except when just using a single Gigabit port on the pluggable module as the source port.

  This is a cosmetic issue and the workaround is to use the **show platform monitor session** privileged EXEC command to display the correct source ports. (CSCtn67868)

Spanning Tree Protocol

- 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.

VLANs

- Integrated Service Router ISR-44X1 have reserved a set of VLANs (2350 to 2449) for additional usage. You must ensure that these VLANs are not used in the network. If the reserve vlans are present in the database, you must remove these reserve vlans before inserting the ISR-44X1 platform. If reserved vlans are present in vlan database of the switch, the module will not come up in ISR-44X1 platforms due to internal vlan allocation failure.

  It is not allowed to add the reserved vlans into vlan database and apply on the front panel ports of the module once the NGIO control path is up. The module will drop the packets if it is tagged with any of the reserved vlans on the front panel ports.

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)

- When the domain is authorized in the guest VLAN on a member switch port without link loss and an Extensible Authentication Protocol over LAN (EAPOL) is sent to an IEEE 802.1x supplicant to authenticate, the authentication fails. This problem happens intermittently with certain stacking configurations and only occurs on the member switches.

  The workaround is to enter the **shut** and **no shut** interface configuration commands on the port to reset the authentication status. (CSCsf98557)

- The error message `%DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND` might appear for a switch stack under these conditions:
  - IEEE 802.1 is enabled.
  - A supplicant is authenticated on at least one port.
  - A new member joins a switch stack.

  You can use one of these workarounds:
  - Enter the **shutdown** and the **no shutdown** interface configuration commands to reset the port.
  - Remove and reconfigure the VLAN. (CSCsi26444)

- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- When 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)

TrustSec

The following guidelines and limitations apply to configuring Cisco TrustSec SGT and SGACL on the Catalyst 3560-X switch:

- You cannot statically map an IP-subnet to an SGT. You can only map IP addresses to an SGT. When you configure IP address-to-SGT mappings, the IP address prefix must be 32.
- If a port is configured in Multi-Auth mode, all hosts connecting on that port must be assigned the same SGT. When a host tries to authenticate, its assigned SGT must be the same as the SGT assigned to a previously authernticated host. If a host tries to authenticate and its SGT is different from the SGT of a previously authenticated host, the VLAN port (VP) to which these hosts belong is error-disabled.
- Cisco TrustSec enforcement is supported only on up to eight VLANs on a VLAN-trunk link. If there are more than eight VLANs configured on a VLAN-trunk link and Cisco TrustSec enforcement is enabled on those VLANs, the switch ports on those VLAN-trunk links will be error-disabled.
- The switch cannot assign an SGT based on SXP listening; it can only forward the SXP bindings through the SXP protocol.
- Port-to-SGT mapping can be configured only on Cisco TrustSec links (that is, switch-to-switch links). Port-to-SGT mapping cannot be configured on host-to-switch links.

  When port-to-SGT mapping is configured on a port, an SGT is assigned to all ingress traffic on that port. There is no SGACL enforcement for egress traffic on the port.

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 launch.

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

Important Notes

Control Plane Protection

Cisco enhanced EtherSwitch service modules internally support up to 16 different control plane queues. Each queue is dedicated to handling specific protocol packets and is assigned a priority level. For example, STP, routed, and logged packets are sent to three different control plane queues, which are prioritized in corresponding order, with STP having the highest priority. Each queue is allocated a certain amount of processing time based on its priority. The processing-time ratio between low-level functions and high-level functions is allocated as 1-to-2. Therefore, the control plane logic dynamically adjusts the CPU utilization to handle high-level management functions as well as punted traffic (up to the maximum CPU processing capacity). Basic control plane functions, such as the CLI, are not overwhelmed by functions such logging or forwarding of packets.

Cisco IOS Notes

- Unlike other platforms, the response to an Energywise query on a 3560-X is the actual switch power consumption and not a fixed number.
- If the switch 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 and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.
- If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software, when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

  ```
  AutoQoS Error: ciscophone input service policy was not properly applied
  policy map AutoQoS-Police-CiscoPhone not configured
  ```

  If this happens, enter the **no auto qos voip cisco-phone** interface command on all interface with this configuration to delete it. Then enter the **auto qos voip cisco-phone** command on each of these interfaces to reapply the configuration.

Device Manager Notes

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch 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 speed up 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. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

  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

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, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch 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 IP information.

- 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 caveats apply to Cisco enhanced EtherSwitch service modules SM-X-ES3-16-P, SM-X-ES3-24-P, and SM-X-ES3D-48-P:

- CSCte99366

  In a Smart Install network, when the director is connected between the client and the DHCP server and the server has options configured for image and configuration, then the client does not receive the image and configuration files sent by the DHCP server during an automatic upgrade. Instead the files are overwritten by the director and the client receives the image and configuration that the director sends.

  Use one of these workarounds:

  – If client needs to upgrade using an image and configuration file configured in the DHCP server options, you should remove the client from the Smart Install network during the upgrade.

  – In a network using Smart Install, you should not configure options for image and configuration in the DHCP server. For clients to upgrade using Smart Install, you should configure product-id specific image and configuration files in the director.

- CSCtn46265

  When you enter the **copy running-config startup config** privileged EXEC command on the switch, the running configuration is not always saved to the startup configuration on the first attempt.

  There is no workaround. If you wait for a few minutes, the configuration is saved when the switch attempts it again.

- CSCtq22963

  NetFlow traffic export fails when the source interface IP address and destination IP address are on different subnets.

  There is no workaround.

- CSCtq38500

  When you configure port-based QoS with an ACL by using the ACL range option, problems can occur if you have also configured **mls qos trus**t on the interface.

  The workaround is to match traffic by using the single port equal (**eq**) option or to not configure **mls qos trust** on the interface.

- CSCtq76989

  A *seed* switch is connected to a RADIUS server either directly or through a trunk port. A *non-seed switch* authenticates with the RADIUS server through the *seed* switch, based on the credential information defined in the RADIUS server. Cisco TrustSec (CTS) parameters must be configured on both the *seed* switch and the *non-seed* switch trunk interfaces.

Although the *non-seed* switch is authenticated and authorized to connect to the network, supplicant devices connected to the *non-seed* switch might be unable to connect to the network, under these circumstances:

- CTS caching is enabled on the *seed* switch and not enabled on the *non-seed* switch.
- The *seed* switch reported the 802.1x role of the *non-seed* switch CTS trunk as authenticator in multi-host mode.
- The *non-seed* switch reported this CTS trunk as the 802.1x authenticator role in single host mode and as supplicant.

The workaround is to reduce the reauthentication time on the *seed* switch, or enter the **shutdown** interface configuration command, followed by the **no shutdown** interface configuration command on the *seed* switch CTS trunk interface.

- CSCtr87645

  ASP now uses a device classifier, which determines the type of device that is connected to the switch. As a result, ASP has no control over the protocol type that is used to detect the device. Therefore, the protocol detection controls are deprecated. When you enter the **macro auto global control detection** command, the protocol does not show up in the running configuration; however, the **filter-spec** command is shown in the output.

  There is no workaround. To see the deprecated commands, enter the **show running config deprecated** global and interface configuration command.

- CSCts75641

  RIP hellos get triplicated as they exit a dot1q-tunnel interface. This situation occurs specifically when a dot1q-tunnel configuration is applied.

  There is no workaround.

- CSCtt22566

  Monitored SPAN traffic is not sent to the SPAN destination when TrustSec MACsec is enabled on the SPAN source interface.

  There is no workaround.

- CSCtz87828

  When a cross-stack Etherchannel is used and one of its link is brought down or up, a MAC address learned from this port-channel may either be prematurely cleared from the table or not aged out.

  The workaround is to use a single switch Etherchannel or to clear dynamically-learned MAC addresses after links have been added to or removed from the channel.

- CSCua22035

  The following message may be erroneously displayed during the boot up process.

  ```
  Message "stack locked up.. even after FSM reset"
  ```

  There is no workaround.

- CSCua29090

  Tracebacks appear during the boot up process.

  There is no workaround.

- CSCua58659

  The global **power inline consumption default 15400** command fails to restrict the power consumption of a PoE+ port 15.4 W.

The workaround is to use the **power inline consumption 15400** command in interface configuration mode.

- CSCua74302 (modules running the LAN base image)

  ACLs applied to outbound traffic on the switch virtual interface (SVI) do not work.

  There is no workaround.

- CSCuc20819

  Errors occur when configuring Cisco Trust Security (CTS) MACsec on the C3KX-SM-10G network service module.

  The workaround is to use the **default** command in CTS manual interface configuration mode to clear the interface, and then reapply the configuration.

- CSCug81202

  When the **show sdm prefer** command is run on the switch, the template displays the number of indirect IPv4 routes as 7.875K instead of 8K compared to Cisco IOS Release 15.0(2)SE2. There is a reduction of 0.125K in the desktop routing template.

  There is no workaround.

- CSCui76579

  When switch is reloaded, total inline power available shows zero.

  There is no workaround.

- CSCum04362

  Switch service module reloads or goes to out-of-service state when IP routing is disabled at line rate. There is no workaround.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 15.0(2)EJ1

Caveats Resolved in Cisco IOS Release 15.0(2)EJ1

- CSCui24617

  When switch is reloaded, ports go to power-deny state.

  There is no workaround.

- CSCuj16336

  Security Group Access Control List (SGACL) is not supported on the service modules even though the corresponding show commands are present.

  There is no workaround.

- CSCuj20123

  When **show hardware led** command is run on the service modules the power LED status is not displayed.

  There is no workaround.

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.

Documents with complete information about the switch are available from these Cisco.com sites:

Catalyst 3560-X
http://www.cisco.com/en/US/products/ps10744/tsd_products_support_series_home.html

Documents with complete information about the EtherSwitch service modules are available from these Cisco.com sites:

- *Connecting Cisco Enhanced EtherSwitch Service Modules to the Network*: http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/eesm_hw.html
- *Cisco Enhanced EtherSwitch Service Modules Configuration Guide*: http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/eesm_sw.html

These documents provide complete information about the EtherSwitch service modules:

- *Cisco SM-X Layer 2/3 EtherSwitch Service Module Configuration Guide for Cisco 4451-X ISR*
- *Cisco SM-X Layer 2/3 EtherSwitch Service Module (ESM) Configuration Guide for Cisco 2900 and Cisco 3900 Series ISRs*

These documents provide complete information about the switches:

- *Release Notes for the Catalyst 3750-X. Catalyst 3750-E, Catalyst 3560-X, and 3560-E Switches*
- *Catalyst 3750-X and 3560-X Switch Software Configuration Guide*
- *Catalyst 3750-X and 3560-X Switch Command Reference*
- *Catalyst 3750-X, 3750-E, 3560-X, and 3560-E Switch System Message Guide*
- *Cisco IOS Software Installation Document.*
- *Catalyst 3750-X and 3560-X Switch Getting Started Guide*
- *Catalyst 3750-X and 3560-X Switch Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Catalyst 3750-X and 3560-X Switch*
- *Installation Notes for the Catalyst 3750-X and 3560-X Switch Power Supply Modules*
- *Installation Notes for the Catalyst 3750-X and 3560-X Switch Fan Module*
- *Installation Notes for the Catalyst 3750-X and 3560-X Switch Network Modules*
- *Cisco Software Activation and Compatibility Document*
- *Auto Smartports Configuration Guide*
- *Cisco EnergyWise Configuration Guide*
- *Smart Install Configuration Guide*
- Information about Cisco SFP, SFP+, and GBIC modules is available from this Cisco.com site: http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

  SFP compatibility matrix documents are available from this Cisco.com site: http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

  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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Obtaining Documentation and Submitting a Service Request" section.