Cisco SM-X Layer 2/3 EtherSwitch Service Module Configuration Guide for Cisco 4451-X ISR

Feb 26, 2016

The Cisco SM-X Layer 2/3 EtherSwitch Service Module (Cisco SM-X Layer 2/3 ESM) integrates the Layer 2 and Layer 3 switching features and provides the Cisco 4451-X ISR the ability to use the Cisco SM-X Layer 2/3 ESM as an independent Layer 3 switch when running the Cisco IOS software.

The Cisco SM-X Layer 2/3 ESMs also provide a 1-Gbps connection to the multigigabit fabric (MGF) for intermodule communication without burdening your router's CPU.

The Cisco SM-X Layer 2/3 ESMs are capable of providing up to 30 watts of power per port with the robust Power over Ethernet Plus (PoE+) feature, along with IEEE 802.3AE Media Access Control Security (MACSec) port-based, hop-to-hop, encryption, and Cisco TrustSec (CTS) which work on multiple router families.

The following is the feature history for the Cisco SM-X Layer 2/3 ESM:

Table 1 Feature History for Cisco SM-X Layer 2/3 ESM

Release	Modification
Cisco IOS XE Release 3.11S (router software) Cisco IOS XE Release 3.10.3S (router software) Cisco IOS Release 15.0(2)EJ1 (switch software)	Support for SM-X-ES3D-48-P was added.
Cisco IOS XE Release 3.10.3S (router software) Cisco IOS XE Release 3.11.2S (router software) Cisco IOS XE Release 3.12.1S (router software) Cisco IOS XE Release 3.13S (router software) Cisco IOS Release 15.2(2)E (switch software) Cisco IOS Release 15.2(3)E (switch software)	Support for 15.2(2)E switch image was released. Support for 15.2(3)E switch image was released.
Cisco IOS XE Release 3.15S (router software)	SVI interface supported on router side was added.

Finding Support Information for Platforms and Cisco IOS Software Images

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Prerequisites for the Cisco SM-X Layer 2/3 EtherSwitch Service Module

The Cisco IOS version on the Cisco SM-X Layer 2/3 EtherSwitch Service Modules must be compatible with the Cisco IOS software release and feature set on the router. See Table 1.

- To view the router (Cisco 4451-X ISR), Cisco IOS software release, and feature set, enter the **show version** command in privileged EXEC mode.
- To view the Cisco SM-X Layer 2/3 ESM IOS XE version, enter the **show platform software subslot** *slot/bay* **module firmware** command in privileged EXEC mode.
- To view the Cisco IOS Release number mapping, see *Release Notes for the Cisco ISR 4400 Series.*

Information About the Cisco SM-X Layer 2/3 EtherSwitch Service Module

This section describes the features and some important concepts about theCisco SM-X Layer 2/3 ESM:

Note For a list of Cisco IOS switch feature documentation with information on various supported features on your Cisco SM-X Layer 2/3 ESM, see the Related Documentation, page 33

Hardware Overview

Cisco SM-X Layer 2/3 ESM are modules to which you can connect devices such as Cisco IP phones, Cisco wireless access points, workstations, and other network devices such as servers, routers, and switches.

The Cisco SM-X Layer 2/3 EtherSwitch Service Module can be deployed as backbone switches, aggregating 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet traffic from other network devices.

The following Cisco enhanced EtherSwitch service modules are available:

- SM-X-ES3-16-P—16-port 10/100/1000 Gigabit Ethernet, PoE+, MAC-Sec enabled Service Module single-wide form factor
- SM-X-ES3-24-P—24-port 10/100/1000 Gigabit Ethernet, PoE+, MAC-Sec enabled Service Module, single-wide form factor
- SM-X-ES3D-48-P—48-port, 10/100/1000 Gigabit Ethernet, 2 SFP Ports, PoE+, MACSec enabled Service Module, double-wide form factor

For complete information about the Cisco SM-X Layer 2/3 ESMs hardware, see the *Connecting Cisco SM-X Layer 2/3 ESMs to the Network* guide.

Software Features

The following are the switching software features supported on the Cisco SM-X Layer 2/3 ESM:

Cisco TrustSec Encryption

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in the cloud is authenticated by its neighbors. Communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. Cisco TrustSec also uses the device and user identification information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. See *Configuring Cisco TrustSec* chapter in the *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later.*

IEEE 802.1x Protocol

The IEEE 802.1x standard defines a client/server-based access control and authentication protocol that prevents clients from connecting to a LAN through publicly accessible ports unless they are authenticated. The authentication server authenticates each client connected to a port before making available any services offered by the router or the LAN.

Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic can pass through the port. See *Configuring IEEE 802.1x Port-Based Authentication* chapter in the *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later.*.

Licensing and Software Activation

The Cisco SM-X Layer 2/3 ESM utilizes the Cisco licensing software activation mechanism for different levels of technology software packages. This mechanism is referred to as technology package licensing and leverages the universal technology package based licensing solution. A universal image containing all levels of a software package is loaded on your Cisco SM-X Layer 2/3 ESM. During startup, the Cisco SM-X Layer 2/3 ESM determines the license according to the license boot level or license priority and loads the corresponding software features.
The Cisco SM-X Layer 2/3 ESM has a right to use (RTU) license, also known as honor-based license.
The RTU license on Cisco SM-X Layer 2/3 ESM supports the following three feature sets:

- LAN Base: Enterprise access Layer 2 switching features
- IP Base: Enterprise access Layer 3 switching features
- IP Services: Advanced Layer 3 switching (IPv4 and IPv6) features

Installing and Applying an RTU License on a Switch

To apply an RTU license on a switch, follow these steps:

Step 1 Upgrade from one license level to another by using the Cisco sales ordering tool to purchase the license. You will receive an e-mail or paper confirmation that grants you permission to install and activate the license on your switch.

Step 2 If you get a license file, use **license install** *stored-location-url* command to install the license. Accept the end-user license agreement when prompted and restart the device to enable the new feature set.

Step 3 Apply the license by entering the appropriate commands on your switch. If you are upgrading a license on a switch, use **license right-to-use activate** ***license-level*** command to activate the higher license. If you are moving a license from one switch to another, use the **license right-to-use deactivate** ***license-level*** command to deactivate the license on the first switch and the activation command on the second switch.

Step 4 Read and accept the End User License Agreement (EULA).

Step 5 Use **show license** command to check the license status.

Step 6 Configure the license boot level to the license you want to use by entering **(config)#license boot level** ***license-level*** command and then save the configuration using **write memory** command.

Step 7 Use **show version** command to check whether the next reload license is correctly configured.

Step 8 Reboot the switch to boot with the highest available license.

See *Upgrading your License Using Right-To-Use Features* for more information on licensing and software activation.

MACsec Encryption

Media Access Control Security (MACsec) encryption is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. MACsec encryption is defined in 802.1AE to provide MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP) framework. Only host facing links (links between network access devices and endpoint devices such as a PC or IP phone) can be secured using MACsec.
The Cisco SM-X Layer 2/3 ESM supports 802.1AE encryption with MACsec Key Agreement (MKA) on downlink ports for encryption between the module and host devices. The module also supports MACsec link layer switch-to-switch security by using Cisco TrustSec Network Device Admission Control (NDAC) and the Security Association Protocol (SAP) key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional) See, “Configuring MACsec Encryption” chapter in the *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later* for information on configuring this feature.

Power over Ethernet (Plus) Features

The Cisco SM-X Layer 2/3 ESM is capable of providing power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices (PDs) from Power over Ethernet (PoE)-capable ports when the switch detects that there is no power on the circuit. The ESM supports IEEE 802.3at (PoE+), which increases the available power for PDs from 15.4 W to 30 W per port. For more information, see the *Power over Ethernet Ports*. The PoE plus feature supports the Cisco discovery protocol (CDP) with power consumption reporting and allows the PDs to notify the amount of power consumed. The PoE plus feature also supports the Link layer discovery protocol (LLDP).

Cisco Intelligent Power Management

The PDs and the switch negotiate power through CDP messages for an agreed power-consumption level. The negotiation allows high-power Cisco PDs to operate at their highest power mode.
The PoE plus feature enables automatic detection and power budgeting; the switch maintains a power budget, monitors, and tracks requests for power, and grants power only when it is available. See the *Configuring the External PoE Service Module Power Supply Mode* section in the *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later.*

Power Policing (Sensing)

Power policing allows to monitor the real-time power consumption. On a per-PoE port basis, the switch senses the total power consumption, polices the power usage, and reports the power usage. For more information on this feature, see Monitoring Real-Time Power Consumption (Power Sensing), page 18.

Managing the Cisco SM-X Layer 2/3 ESM Using Cisco IOS Software

This sections contains the following topics with information on managing the Cisco SM-X Layer 2/3 ESM on the Cisco 4451-X ISR using Cisco IOS software:

Using OIR to Manage the Cisco SM-X Layer 2/3 ESM

The online insertion and removal (OIR) feature allows you to insert or remove your Cisco SM-X Layer 2/3 ESM from a Cisco 4451-X ISR without powering down the module. This process is also referred to as a surprise or hard OIR. When performing a surprise OIR, you must save all your configuration on the ESM; any unsaved configuration will be lost during a surprise OIR. The Cisco 4451-X ISR also supports any-to-any OIR, which means that a service module (SM) in a slot can be replaced by another SM using the OIR feature.

When a module is inserted, power is available on the ESM, and it initializes itself to start functioning. The hot-swap functionality allows the system to determine when a change occurs in the unit's physical configuration and to reallocate the unit's resources to allow all interfaces to function adequately. This feature allows interfaces on the ESM to be reconfigured while other interfaces on the router remain unchanged. The software performs the necessary tasks involved in handling the removal and insertion of the ESM.

You can choose to gracefully power down your Cisco SM-X Layer 2/3 ESM before removing it from router. This type of OIR is also known as managed OIR or soft OIR. The managed OIR feature allows you to stop the power supply to your module using the **hw-module subslot [stop]** command and remove the module from one of the subslots while other active modules remain installed on the router.

Note If you are not planning to immediately replace a module after performing OIR, ensure that you install a blank filter plate in the subslot.

The **stop** option allows you to gracefully deactivate a module; the module is rebooted when the **start** option of the command is executed. The **reload** option will stop or deactivate a specified module and restart it. See the Shutting Down and Reloading the Cisco SM-X Layer 2/3 ESM for more information.

Preventing ESM from Automatic Reloads

The Cisco 4451-X ISR monitors the module status and recovers the module by reloading it when there is a failure. After initiating a reload, router waits for 7 minutes for the module to be in an “OK” state. If the module does not come to an “OK” state within these 7 minutes, the router considers this as a failure and retries the recovery process. The maximum number of retry attempts that the router can make is 5. After 5 such attempts, if the module does not come back to an “OK” state, the router puts the module in an “Out of Service” state and terminates the error recovery process.

This behavior may create a problem in certain processes where booting a Cisco SM-X Layer 2/3 ESM may take more than 7 minutes. For example, when booting the Cisco SM-X Layer 2/3 ESM with a new IOS switch release, there can be microcode upgrade on the Cisco SM-X Layer 2/3 ESM by the new Cisco IOS image. In such situations, prevent the router from automatically reloading the module after 7 minutes by disabling error recovery on a particular subslot. You can prevent the router from reloading by enabling the maintenance mode. See the Enabling Maintenance Mode, page 7 for more information.

Once the module is placed into maintenance mode, you can bring it back into the normal operational mode using the **hw-module subslot** *x/0* **reload** command.

Enabling Maintenance Mode

We recommend that you enable the maintenance mode on the switch module when booting the module with a new software image that requires bootloader upgrade and takes more than 7 minutes. Use the **hw-module subslot** *X/0* **maintenance enable** command to enable the maintenance mode. Enabling the maintenance mode allows the switch module to take more than the default time limit of 7 minutes to boot. When you fail to configure maintenance mode, the OIR timeout requests the module to go again for reload. The switch module will be up and displayed as “out of service” in the **show platform** command output on the host router but it remains operational. You can disable the maintenance mode using the **hw-module subslot** *X/0* **maintenance disable** command. Reload the module again to bring-up the connection between the host router and the module.

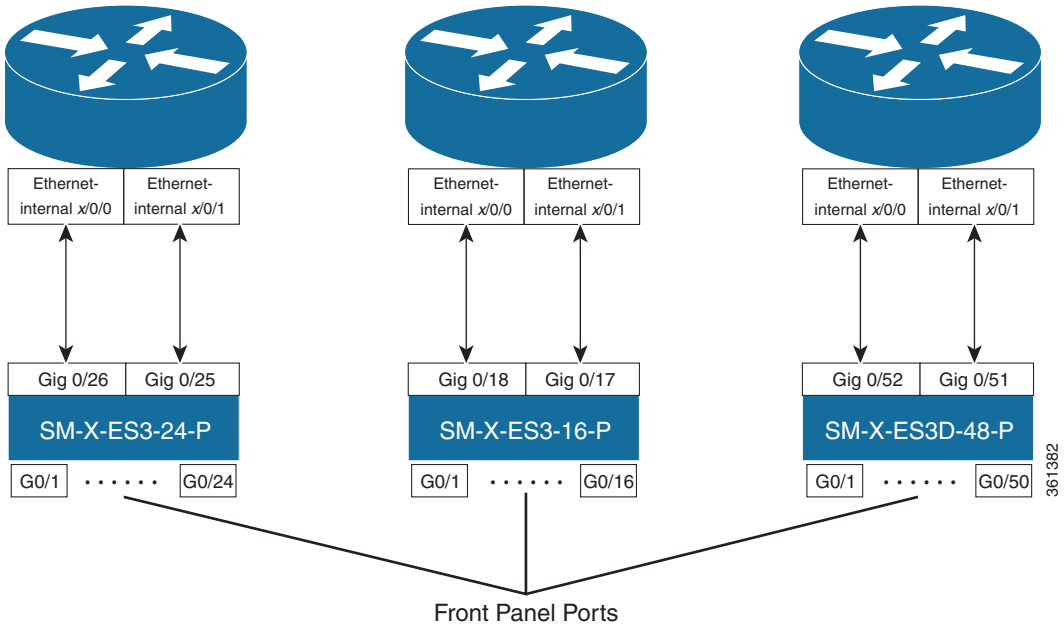
Internal VLAN 2351

VLAN 2351 is an internal VLAN used for SM-X layer2/3 ESM and Cisco 4451-X ISR communication. VLAN 2351 configuration is temporarily added during the module boot up and will be removed after module boots up successfully. If this configuration is shown up under SM-X layer2/3 ESM uplink port, it means that the ESM module does not come up correctly and module is not in service. Make sure that all necessary steps are followed described in 'Upgrading the Cisco SM-X layer2/3 ESM Software' section and reboot the ESM module.

Internal Port Mapping

Figure 1 below displays the internal port mapping between the Cisco SM-X Layer 2/3 ESM and the Cisco 4451-X ISR. The variable "x" indicates the slot number where the Cisco SM-X-ES3-16-P, Cisco SM-X-ES3-24-P and Cisco SM-X-ES3D-48-P SKUs of the module are inserted on the Cisco 4451-X ISR router.

Figure 1 Port Mapping for Cisco SM-X Layer 2/3 ESM on Cisco 4451-X ISR



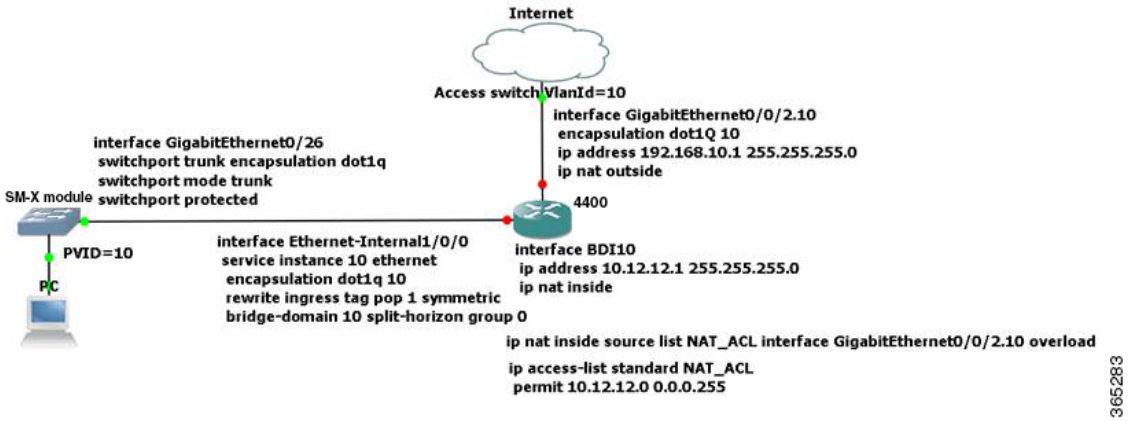
Managing MGF Ports for Layer 2 Features

The Cisco SM-X Layer 2/3 ESM enables the backplane Ethernet interfaces using the **interface Ethernet-internal** *slot* **/0/[0|1]** command to ensure proper management of Layer 2 switching properties such as access, trunk, and dynamic mode of its two MGF ports, GE0 and GE1. The MGF port uses certain switchport commands to perform different functions for different modes. For example, access mode is used for end devices; trunk mode is used for lines between switches and other lines that send multiple VLANs over a single connection, and dynamic mode automatically detects what kind of device is connected and initiates its port accordingly.

Enabling Layer-3 Features under Ethernet-internal Interface

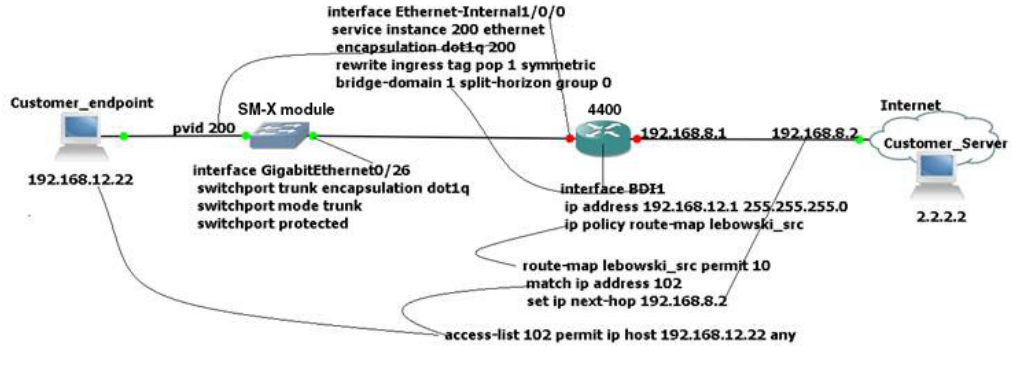
The following examples show the Layer 3 feature configuration. In Figure 2, you should configure **ip nat inside** under the BDI10 instead of configuring it under interface Ethernet-internal1/0/0.

Figure 2 Layer 3 Feature Configuration



In Figure 3, you should configure PBR under BDI1 instead of configuring it under interface Ethernet-internal1/0/0.

Figure 3 Layer 3 Feature Configuration



How to Configure the Cisco SM-X Layer 2/3 ESM on the Router

The SM-X configuration includes SM-X module side configuration and host side configuration. The SM-X module's configuration is the same as common C3560E switch. To configure layer 3 features (For example HSRP, PBR and Nat etc), you can configure it on host side BDI or SVI interfaces on host side. Layer 3 sub-interface is represented by different BDI/SVI interface on host side.

Configuration on SM-X Module Side

- Configuration: Known Issues, page 11

Accessing SM-X Module Side Through a Console Connection or Through Telnet

Before you can access the modules, you must connect to the host router through the router console or through Telnet. Once you are connected to the router, ope a session to your module using the **hw-module session** command in privileged EXEC mode.

You can use the following method to establish a connection to the module:

Connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router.

You can use the following configuration examples to establish a connection:

Step 1 Open a session from the router using the following command:

Example:

```
Router# hw-module session 1/0
Establishing session connect to subslot 1/0
To exit, type ^a^q

picocom v1.4

port is        : /dev/ttyDASH0
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : ascii_xfr -s -v -l10
receive_cmd is : rz -vv

Terminal ready

Switch#
```

Step 2 Exit the session from the switch, press **Ctrl-a** and **Ctrl-q** from your keyboard:

Example:

```
Switch# <type ^a^q>
Thanks for using picocom
Router#
```

Understanding Interface Types on the Cisco SM-X Layer 2/3 ESMs

The Cisco SM-X Layer 2/3 ESM supports the following types of interfaces:

- Ethernet internal interfaces on the host
- Gigabit Ethernet interfaces on the module
- VLAN switched virtual interface (SVI) on the module

Using Interface Configuration Mode

You can configure the individual Cisco SM-X Layer 2/3 ESM physical interfaces (ports) through interface configuration mode on the CLI.

- Type—GigabitEthernet (gigabitethernet or gi) for 10/100/1000-Mbps Ethernet ports.
- Module number—The module slot number on the Cisco SM-X Layer 2/3 ESM or switch (always 0 on the service module or switch).
- Port number—The interface number on the Cisco SM-X Layer 2/3 ESM or switch. The port numbers always begin at 1, starting at the left side of the Cisco SM-X Layer 2/3 ESM, for example, interface GigabitEthernet 0/1.

You can identify physical interfaces by physically checking the interface location on the Cisco SM-X Layer 2/3 ESM. You can also use the Cisco IOS **show** privileged EXEC commands to display information about a specific interface or all the interfaces on the Cisco switching service module.

Example

To specify Gigabit Ethernet port 4 on a standalone Cisco SM-X Layer 2/3 ESM, enter this command in global configuration mode:

```
Switch(config)# interface GigabitEthernet 0/4
```

Configuration: Known Issues

mls qos configuration notes

If mls qos is configured, the QoS configuration must reserve resource for the internal traffic. The basic idea of the module QoS egress buffering scheme is that each port with its 4 egress queues (queue1 to queue 4) are initially allocated a certain number of buffers. Each queue has three drop thresholds. The module internal traffic makes use of queue 2 threshold 3.

Configure shutdown command notes

If you configure the **shutdown** command on the module to module interface (Gi0/17 for SM-X-ES3-16-P, Gi0/25 for SM-X-ES3-24-P, Gi0/51 for SM-X-ES3D-48-P), after the module reloads, the interface configuration resets to **no shutdown**. This example shows the interface configuration:

```
Device (config)# interface Gi0/25
Device (config-if)# shutdown
Interface configuration is:
interface GigabitEthernet0/25
switchport protected
shutdown
end
```

After save configuration and reload module, the configuration is reset to

```
interface GigabitEthernet0/25
switchport protected
end
```

Configuration on Host Side

Configuring BDI

The BDI interface on router side that is used for module and router traffic is Layer 3. To prevent loops from occurring when more than one module is configured with same bridge domain interface, you must configure the same bridge domain with **split-horizon** to stop the traffic flow between the two modules as shown below:

You can also configure the layer-3 features in BDI interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface Ethernet-Internal**1/0/0
3. **service instance** *1* **ethernet**
4. **encapsulation dot1q** *20*
5. **rewrite ingress** *tag pop 1* **symmetric**
6. **bridge-domain** 1 **split-horizon** *group 0*
7. **interface Ethernet-Internal** 2/0/0
8. **service instance** *1 ethernet*
9. **encapsulation dot1q** *20*
10. **rewrite ingress** *tag pop 1* **symmetric**
11. **bridge-domain** 1 **split-horizon** *group 0*
12. **interface BDI** 1

13. **mtu** *9216*
14. **ip address** 10.0.0.1 255.255.255.0

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface Ethernet-Internal** *slot/0/0* **Example:** `Router(config)# interface Ethernet-Internal 1/0/0`	Configures the Cisco SM-X Layer 2/3 EtherSwitch Service Module.
Step 3	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 1 ethernet`	Creates a service instance on an interface and enters service instance configuration mode.
Step 4	**encapsulation** *vlan id* dot1q [second-dot1q *vlan id*] **Example:** `Router(config-if-srv)# encapsulation dot1Q 10`	Defines the encapsulation type and enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN. • vlan-id — Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID. • native — (Optional) Sets the VLAN ID value of the port to the value specified by the vlan-id argument. **Note** This keyword is not supported by the IEEE 802.1Q-in-Q VLAN Tag Termination feature. • second-dot1q — Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature by allowing an inner VLAN ID to be configured. • any — Sets the inner VLAN ID value to a number that is not configured on any other subinterface. **Note** The any keyword in the second-dot1q command is not supported on a subinterface configured for IP over Q-in-Q (IPoQ-in-Q) because IP routing is not supported on ambiguous subinterfaces.

	Command or Action	Purpose
Step 5	**rewrite ingress tag pop symmetric** **Example:** `Router(config-if-srv)#rewrite ingress tag pop 1 symmetric`	Specifies the tag manipulation that is to be performed on the frame ingress to the service instance. **Note** If this command is not configured, then the frame is left intact on ingress (the service instance is equivalent to a trunk port).
Step 6	**bridge-domain** *vlan id* **split-horizon** *id* **Example:** `Router(config-if-srv)# bridge-domain 1 split-horizon group 0`	Enables RFC 1483 split horizon mode to globally prevent bridging.
Step 7	**interface Ethernet-Internal** *slot* /0/0 **Example:** `Router(config)# interface Ethernet-Internal 2/0/0`	Configures the second Cisco SM-X Layer 2/3 ESM (ESM1).
Step 8	**service instance** *id* **ethernet** **Example:** `Router(config-if)# service instance 1 ethernet`	Creates a service instance on an interface and enters service instance configuration mode.
Step 9	**encapsulation** *vlan id* dot1q [second-dot1q *vlan id*] **Example:** `Router(config-if-srv)# encapsulation dot1q 20`	Defines the encapsulation type and enables IEEE 802.1Q encapsulation of traffic on a specified subinterface in a VLAN. See details in Step 4
Step 10	**rewrite ingress tag pop symmetric** **Example:** `Router(config-if-srv)# rewrite ingress tag pop 1 symmetric`	Specifies the tag manipulation that is to be performed on the frame ingress to the service instance. **Note** If this command is not configured, then the frame is left intact on ingress (the service instance is equivalent to a trunk port).
Step 11	**bridge-domain** *vlan id* **split-horizon** *id* **Example:** `Router(config-if-srv)# bridge-domain 1 split-horizon group 0`	Enables RFC 1483 split horizon mode to globally prevent bridging.
Step 12	**interface BDI** *interface number* **Example:** `Router(config)# interface BDI 1`	Specifies a bridge domain interface.

Command or Action	Purpose
Step 13 **mtu** *bytes* **Example:** `Router(config-if)# mtu 9216`	Configures the MTU size for the interface VLAN. • bytes—The range is 64 to 9216; the default is 1500.
Step 14 **ip address** *ip address* **Example:** `Router(config-if)# ip address 10.0.0.1 255.255.255.0`	Configures the IP address.

Configuring SVI Interface

Starting from Cisco IOS XE Release 3.15S, Cisco ISR4000 routers support SVI (Switch Virtual Interface). SVI configuration and association to Ethernet-internal x/0/0 interface on router side is needed. Enabling or disabling SVI configuration under switch-internal interface needs a module OIR or router reload after configuration was saved.

You can also configure Layer-3 features in SVI interface.

The following example shows the router configuration:

```
router#configure terminal
router (config)#ethernet-internal subslot 1/0
router(config-ether-internal)# platform switchport svi
router(config-ether-internal)#exit
router(config)#vlan 601
router(config-vlan)#exit
route(config)#interface Ethernet-Internal 1/0/0
router(config-if)#switchport mode trunk
router(config-if)#switchport trunk allowed vlan 601
router(config-if)#exit
router(config)#interface vlan 601
router(config-if)#ip address 10.0.0.1 255.255.255.0
```

Configuration: Known Issues

HSRP configuration notes

BDI requires support of APPXk9 license on ISR 4000 routers for pre 15.5(3)S releases.

Shutting Down and Reloading the Cisco SM-X Layer 2/3 ESM

You can shut down or deactivate your module using the OIR feature, by executing the **hw-module subslot shutdown** command in global configuration mode. When using the **hw-module subslot shutdown** command, you can choose to put your module in unpowered state. **Unpowered** state shuts down the module and removes power from the module. Use this option when you plan to remove the module from the chassis.

If you choose to deactivate your module and its interfaces by executing the **hw-module subslot shutdown** command in global configuration mode, you are able to change the configuration in such a way that no matter how many times the router is rebooted, the module does not boot. This command is

useful when you need to shut down a module located in a remote location and ensure that it does not boot automatically when the router is rebooted.To begin using the interface again, you must manually re-enable the module using the **no hw-module subslot shutdown** command.

Note If you choose to use the **hw-module subslot stop** command in EXEC mode, you cause the module to gracefully shut down. However, the module is rebooted when the **hw-module subslot start** command is executed.

SUMMARY STEPS

1. **hw-module subslot** *slot-number/subslot-number* **shutdown unpowered**
2. **hw-module subslot** *slot-number/subslot-number* [**stop | start| reload**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**hw-module subslot** 1/0 **shutdown unpowered** **Example:** `Router(config)# hw-module subslot 1/0 shutdown unpowered`	Disables the Cisco SM-X Layer 2/3 ESM in in subslot 1/0 without removing the module from the router in global configuration mode.
Step 2	**hw-module subslot** *slot-number/subslot-number* [**reload	stop	start**] **Example:** `Router# hw-module subslot 1/0 stop`	Deactivates the module in the specified slot and subslot in EXEC mode. • *slot-number*—Specifies the chassis slot number where the module is installed. • *subslot-number*—Specifies the subslot number of the chassis where the module is installed. • **reload**— Gracefully stops and reloads the specified module. • **stop**—Stops the specified module. • **start**—Starts the specified module.

Example

This section provides the following examples:

- Sample Output for the hw-module subslot 1/0 shutdown unpowered Command, page 17
- Sample Output for the hw-module subslot slot/subslot reload Command, page 18

Sample Output for the hw-module subslot 1/0 shutdown unpowered Command

The following example shows what appears when you enter the **hw-module subslot** *slot-number/subslot-number* **shutdown** command:

```
Router(config)#hw-module subslot 1/0 shutdown unpowered
Router(config)#
*Jun 21 16:29:13.307 IST: %SPA_OIR-6-SHUTDOWN: subslot 1/0 is administratively shutdown;
Use 'no hw-module  shutdown' to enable
```

```
*Jun 21 16:29:13.308 IST: %SPA_OIR-6-OFFLINECARD: SPA (SM-X-ES3-24-P) offline in subslot
1/0
Router(config)#end
*Jun 21 16:29:35.505 IST: %SYS-5-CONFIG_I: Configured from console by consolehw
```

You can verify the status of the Cisco SM-X Layer 2/3 ESM by issuing the following show command:

```
Router#sh hw-module subslot 1/0 oir
Module        Model                Operational Status
------------- -------------------- ----------------------
subslot 1/0   SM-X-ES3-24-P         admin down
```

Sample Output for the hw-module subslot *slot/subslot* reload Command

The following example shows what appears when you enter the **hw-module subslot** *slot-number/subslot-number* **reload** command:

```
Router# hw-module subslot 1/0 reload
Proceed with reload of module? [confirm]
Router#
*Jun 21 16:32:58.017 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(SM-X-ES3-16-P) reloaded on
subslot 1/0
*Jun 21 16:32:58.018 IST: %SPA_OIR-6-OFFLINECARD: SPA (SM-x-ES3-16-P) offline in subslot
2/0At the confirmation prompt, press Enter to confirm the action or n to cancel.
```

Monitoring Real-Time Power Consumption (Power Sensing)

Cisco SM-X Layer 2/3 ESMs' hardware allows the ESM to accurately monitor the real-time power consumption on each port by measuring the port current as well as the voltage while the powered devices such as IP phones and wireless access points are powered up.

If a powered device is misbehaving by consuming more power than the actual configured value, you can take an appropriate 'action' by enabling the power policing or sensing feature on a port using the **power inline** command. The 'action' is either "logging a warning message" (also knows as lax policing) or shutting down a misbehaving port (strict policing). The ESM constantly monitors the power drawn by the powered devices and takes appropriate action on misbehaving ports. You can monitor the power drawn by the powered devices through **power inline** command.

When power policing is enabled on a port, you can pick a cutoff power value of "x" watts per port and choose an 'action' to be taken on the misbehaving ports. Power policing is disabled by default on all ports.

Note You must take the cable loss into consideration when configuring the power monitoring or power policing value for a given port of the switch. There might be some cable loss while configuring power cutoff value at the PSE. The switch can only police the power drawn at the PSE RJ45 port and not the actual power consumed by the powered device.

Restrictions

- Because the switch can only monitor the power drawn at the PSE RJ45 port and not what the PD actually consumes, you must plan for the worst case cable loss when configuring the power cutoff value.
- When power drawn by the power devices exceeds the maximum limit after a period of 1 second or more, the system considers the ports as, "misbehaving ports" and shuts down the power supply.

SUMMARY STEPS

1. **config terminal**
2. **interface gigabitethernet 0/x**
3. **power inline max** *max-wattage*
4. **power inline police action** *action*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet 0/24`	Enter interface configuration mode and places you at the GigabitEthernet 0/24 interface.
Step 4	**power inline max** *max-wattage* **Example:** `Router(config-if)# power inline max 4000`	Specifies the cut off power value for a port. • **max** *max-wattage*—Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed.
Step 5	**power inline police action** *action* **Example:** `Router(config-if)# power inline police action log`	Enables the ESM to generate a syslog message while still providing power to the device. • **action** *action*— Specifies an action. For example, a log message or a warning message to avoid flooding of event log or even shutting down the port.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits the interface configuration mode.

Example

The following example displays the maximum power configured:

```
Router# show power inline
Available:500.0(w)  Used:24.0(w)  Remaining:476.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Et1/0/0   auto   off        24.0    n/a                n/a   750.0
Et2/0/0   auto   off        0.0     n/a                n/a   750.0
```

The following example shows power consumed by various devices connected to your module:

```
Switch# show power inline
Available:500.0(w)  Used:24.0(w)  Remaining:476.0(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Gi0/1     auto   off        0.0     n/a                n/a   30.0
Gi0/2     auto   on         12.0    IP Phone 7975      3     30.0
Gi0/3     auto   on         12.0    IP Phone 9951      4     30.0
Gi0/4     auto   off        0.0     n/a                n/a   30.0
Gi0/5     auto   off        0.0     n/a                n/a   30.0
Switch# show power inline police
Available:623(w)  Used:6(w)  Remaining:617(w)
Interface Admin  Oper       Admin       Oper         Cutoff Oper
          State  State      Police      Police       Power  Power
--------- ------ ---------- ----------  ----------   ------ -----
Gi0/1     auto   off        none        n/a          n/a    0.0
Gi0/2     auto   on         none        n/a          n/a    16.7
Gi0/3     auto   off        errdisable  n/a          0.0    0.0
Gi0/4     auto   on         errdisable  ok           16.6   11.4
Gi0/5     auto   on         log         ok           16.6   11.2
Gi0/6     auto   on         errdisable  overdrawn    0.0    0.0
```

The following table lists the interface and the status.The following example shows the power usage when PDs (powered devices) are connected to your module:

```
Switch# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
ISR 4451-X       Gig 0/26          150               R    ISR4451-X BDI1
ISR 4451-X       Gig 0/26          172               R    ISR4451-X Eth 1/0/0
SEPE80462EB2EA7  Gig 0/2           155             H P M  IP Phone  Port 1
SEPACA0166EFD07  Gig 0/3           163             H P M  IP Phone  Port 1
```

Upgrading the Cisco SM-X Layer 2/3 ESM Software

This section describes how to upgrade the Cisco SM-X Layer 2/3 ESM software by using TFTP.

You can copy the switch image to the ESM flash by following one of the two methods listed below:

- Establish connectivity from your ESM's front panel port to the TFTP server where the desired switch Cisco.com image is stored. If there is no TFTP server, you can also establish connectivity from your ESM's front panel port to the host side (use as TFTP server) front panel port.
- Copy the switch image (available on Cisco.com) to the router's flash and copy this image to ESM flash through TFTP.

Copying Switch Image Directly to ESM Flash Through TFTP Server

This section describes how to copy a switch image directly to the ESM flash through the TFTP server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *0/x*
4. **no switchport**
5. **ip address** *ip address/subnet mask*
6. **no shutdown**
7. **end**
8. **show run interface gigabitethernet** *0/x*
9. **ping tftp-server-ip-address**
10. **dir flash:**
11. **copy tftp: flash:**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enters privileged EXEC mode.
	Example: `Switch> enable`	
Step 2	**configure terminal**	Enters global configuration mode.
	Example: `Switch# configure terminal`	
Step 3	**interface gigabitethernet** *0/x*	Enter interface configuration mode and places you at the GigabitEthernet 0/24 interface.
	Example: `Switch(config)# interface gigabitethernet 0/24`	
Step 4	**no switchport**	Enables the routed port. **Note** The **no switchport** command is only available on the SM-X Layer3 ESMs.
	Example: `Switch(config-if)# no switchport`	
Step 5	**ip address** *ip address/subnet mask 192.1.10.200 255.255.255.240*	Sets a primary or secondary IP address for this interface.
	Example: `Switch(config-if)# ip address 192.1.10.200 255.255.255.240`	

	Command or Action	Purpose
Step 6	**no shutdown** **Example:** `Switch(config-if)# no shutdown`	Enables the port that is connected to the TFTP server.

Step 7	**end**
	
	Example:
	`Switch(config)# end`
	`Switch#`
		Exits interface configuration mode, and returns to privileged EXEC mode.

Step 8	**show run interface gigabitethernet** *0/x* **Example:** `Switch# show run interface gigabitethernet 0/24`	Shows the configuration applied on this interface.
Step 9	**ping tftp-server-ip-address** **Example:** `Switch# ping 172.16.1.100`	Pings for network connectivity.
Step 10	**dir flash:** **Example:** `Switch# dir flash:`	Displays a list of all files and directories in the Cisco SM-X Layer 2/3 ESM flash memory.
Step 11	**copy tftp: flash:** **Example:** `Switch# copy tftp: flash:`	Copies an image from a TFTP server to flash memory.

Examples

This section provides the following examples:

- Sample Output for the show run interface gigabitethernet Command, page 23
- Sample Output for the ping ip address Command, page 24
- Sample Output for the show flash: Command, page 24
- Sample Output for the copy tftp: flash: Command, page 24

Sample Output for the show run interface gigabitethernet Command

The following example shows what appears when you enter the **show run interface gigabitethernet** command:

```
Switch# show run gigabitethernet 0/24
Building configuration...
Current configuration : 87 bytes
!
interface GigabitEthernet0/24
```

```
 no switchport
 ip address 172.16.1.100 255.255.255.0
end
```

Sample Output for the ping ip address Command

The following example shows what appears when you enter the **ping ip address** command:

```
Switch# ping 172.16.1.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
Copy the image from the tftp server to the switch flash using standard tftp copy
procedure.
```

Sample Output for the show flash: Command

The following example shows what appears when you enter the **dir flash:** command:

```
Switch# dir flash:

Directory of flash:/

2 -rwx 2998 Mar 3 1993 19:26:15 +00:00 express_setup.debug
3 -rwx 20291584 Aug 12 2013 14:51:08 +00:00 c3560e-universalk9-mz
4 -rwx 6168 Mar 30 2011 01:31:04 +00:00 multiple-fs
13 -rwx 3453 Mar 30 2011 01:31:03 +00:00 config.text
6 -rwx 1916 Mar 30 2011 01:31:03 +00:00 private-config.text
8 -rwx 1149 Apr 6 2011 18:05:53 +00:00 FOC163902N0_20130808013323578.lic
9 drwx 4096 Jul 25 2013 06:51:51 +00:00 dc_profile_dir
11 drwx 4096 Mar 30 2011 01:30:06 +00:00 front_end_ucode_cache

88735744 bytes total (67715072 bytes free)
Switch#
```

Sample Output for the copy tftp: flash: Command

The following example shows what appears when you enter the **copy tftp: flash:** command:

```
Switch# copy tftp: flash:

Address or name of remote host []? 172.16.1.100
Source filename []? ciscouser/c3560e-universalk9-mz
Destination filename [c3560e-universalk9-mz]?
Accessing tftp://172.16.1.100/ciscouser/c3560e-universalk9-mz...
Loading ciscouser/c3560e-universalk9-mz from 172.16.1.100 (via GigabitEthernet0/1): !!!!
[OK - 20291584 bytes]

20291584 bytes copied in 113.170 secs (179302 bytes/sec)
Switch#
```

Copying Switch Image to ESM Flash Through Host Router

This section describes how to copy the switch image to the ESM flash through the host router.

Note Both BDI and SVI can be used on the router side. For more information, see: Configuration on Host Side, page 12.

SUMMARY STEPS

Step 1 Prepare switch-image on host side

a. Copy ESM image to router bootflash.

b. Configure host router as TFTP server.

c. Configure terminal and tftp-server bootflash:switch-image

Step 2 Login ESM module side and copy image

a. Login ESM module

b. hw-module session x/0

c. Copy image from host side

The following example shows hoe to copy the siwtch image to the ESM flash through the host router:

```
Router#copy ftp://asr:asr@10.74.5.77:c3560e-universalk9-mz.152-3.E.bin .
Source filename []? c3560e-universalk9-mz.152-3.E.bin
Destination filename [c3560e-universalk9-mz.152-3.E.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing ftp://*:*@10.74.5.77:c3560/c3560e-universalk9-mz.152-3.E.bin...
Loading c3560e-universalk9-mz.152-3.E.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!
[OK - 26306267/4096 bytes]

26306267 bytes copied in 8.246 secs (3190185 bytes/sec)
Router#

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#tftp-server bootflash:c3560e-universalk9-mz.152-3.E.bin

Router#show run | inc 152-3
tftp-server bootflash:c3560e-universalk9-mz.152-3.E.bin

Router#show run int gi0/0/0
interface GigabitEthernet0/0/0
 description connect to SM-X GI0/1 for TFTP connectivity
 ip address 192.168.100.1 255.255.255.0
 media-type rj45
 negotiation auto

Router#hw-module session 1/0
Establishing session connect to subslot 1/0
To exit, type ^a^q

picocom v1.4
```

```
port is        : /dev/ttyDASH0
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : ascii_xfr -s -v -l10
receive_cmd is : rz -vv

Terminal ready

Switch(config)#int gi0/1
Switch(config-if)#switchport access vlan 100
Switch(config-if)#end
Switch#

Switch#show run int gi0/1
Building configuration...

Current configuration : 130 bytes
!
interface GigabitEthernet0/1
 description connected to host side GI0/0/0 for TFTP connectivity
 switchport access vlan 100
end

Switch(config)#int vlan 100
Switch(config-if)#ip addr 192.168.100.2 255.255.255.0
Switch(config-if)#end
Switch#

Switch#show run int vlan 100
Building configuration...

Current configuration : 65 bytes
!
interface Vlan100
 ip address 192.168.100.2 255.255.255.0
end

Switch#copy tftp: flash:
Address or name of remote host [192.168.100.1]?
Source filename [c3560e-universalk9-mz.152-3.1.26.E1.bin]?
c3560e-universalk9-mz.152-3.E.bin
Destination filename [c3560e-universalk9-mz.152-3.E.bin]?
Accessing tftp://192.168.100.1/c3560e-universalk9-mz.152-3.E.bin...
Loading c3560e-universalk9-mz.152-3.E.bin from 192.168.100.1 (via Vlan100):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!
[OK - 26306267 bytes]

26306267 bytes copied in 145.878 secs (180331 bytes/sec)
```

Upgrading SM-X Image

This section describes how to upgrade SM-X image.

SUMMARY STEPS

Step 1 Enable maintenance on host side before upgrade. Run the **hw-module subslot x/0 maintenance enable** command.

Step 2 Copy the image to SM-X module. Run **boot system flash:xxx** command on SM-X module.

Step 3 Make sure that there is no "front_end_ucode_cache" directory on SM-X module. Delete the file if any such file exists.

Step 4 Reload the module. Type **hw-module subslot x/0 reload** command on host side. The upgrade procedure starts after the module bootup. This step is very time consuming. Do not interrupt it.

Step 5 After the module comes up, disable the maintenance on host side using the **hw-module subslot x/0 maintenance disable** command.

Step 6 Reload the SM-X module from the host side again. Note that, Step 4 reload is not enough. Use the **hw-module subslot x/0 reload force** command to reload the module.

The following examples shows the detailed upgrade procedure:

```
Step 1. Router#hw-module subslot 1/0 maintenance enable

Step 2. Reference above copy image section
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#boot system flash:c3560e-universalk9-mz.152-3.E.bin
Switch(config)#end
Switch#
*Jan  4 15:31:03.188: %SYS-5-CONFIG_I: Configured from console by console
Switch#wr
Building configuration...
[OK]

Step 3.
Switch#dir front_end_ucode_cache
%Error opening flash:/front_end_ucode_cache (No such file or directory)

Step 4.
Router#hw-module subslot 1/0 reload
Proceed with reload of module? [confirm]

Step 5. Do not interrupt following time consuming upgrade procedure

Step 6.

Step 7.
```

Module-to-Module Communication

Cisco SM-X Layer 2/3 ESM can directly communicate with any module connected to the backplane switch of the router bypassing the router host CPU, thus, increasing the CPU performance and reducing the CPU processing. The additional GE connection with the router backplane switch designated as **Ethernet-Internal X/0/1** port where **X** is the slot number. This port can be access port or a trunk port.

Example

Following is an example of the configuration assuming a 16 port module is configured in slot 1 and a 24 port module in slot 2:-

```
Configuration on the router:
interface Ethernet-Internal 1/0/1
 switchport access vlan 10
!
interface Ethernet-Internal 2/0/1
 switchport access vlan 10
```

Configuration on the 16 port SM-X module in slot 1:

```
interface gigabitethernet 0/17
 switchport access vlan 10
!
```

Configuration on the 24 port SM-X module in slot 2:

```
interface gigabitethernet 0/25
 switchport access vlan 10
```

You can apply the trunk port configurations if the port needs to be a trunk port.

Troubleshooting the Cisco SM-X Layer 2/3 ESM Software

This section describes how to troubleshoot the Cisco enhanced EtherSwitch service module:

- Recovering from a Corrupted Software Image Using Boot Loader, page 28
- Recovering from a Lost or Forgotten Password, page 29
- Related Documentation, page 33

Recovering from a Corrupted Software Image Using Boot Loader

The Cisco SM-X Layer 2/3 EtherSwitch Service Module software can get corrupted when downloading a wrong file during the software upgrade process and when the image is invalid or even when there is no image available.

The **load_recovery** command allows you to recover from a corrupted software image, an invalid image or no image on the flash of the module.

The **load_ recovery** command boots the ESM with an IOS image (recovery image). Once the module is booted, desired Cisco.com switch image can be copied to the module flash through TFTP from the router's flash or through the ESM front panel switch ports.

Copying a Cisco.com switch image to the ESM flash through module's front panel switch ports only works when there is a connectivity established to the TFTP servers from the front panel ports of your ESM.

Note The router should have the ESM image in the router flash memory or the ESM should have network connectivity to TFTP server through its front panel ports.

Note We recommend that you continue all network operations using the new image and not the recovery image.

To start the load recovery process, issue the **load_recovery** command in bootloader prompt. After you issue the **load_recovery** command, the following message appears:

```
switch: load_recovery
 Loading "rs:/c3560e-universalk9-mz.recovery_04302013"...Verifying image
rs:/c3560e-universalk9-mz.recovery_04302013

Image passed digital signature verification

File "rs:/c3560e-universalk9-mz.recovery_04302013" uncompressed and installed, entry
point: 0x3000
 executing...
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
           cisco Systems, Inc.            170 West Tasman Drive            San Jose,
California 95134-1706

Switch>
```

Now you can upgrade to a new switch image, see the Upgrading the Cisco SM-X Layer 2/3 ESM Software, page 21.

Recovering from a Lost or Forgotten Password

This section shows how to recover from a lost or forgotten password.

The default configuration for the Cisco SM-X Layer 2/3 ESM allows you to recover from a lost password by entering a new password.

During auto boot loader operation, you are not presented with the boot loader command-line prompt. You gain access to the boot loader command line if the switch is set to manually boot or, if an error occurs, the operating system (a corrupted Cisco IOS image) is loaded. You can also access the boot loader if you have lost or forgotten the switch password.

Note The default configuration for Cisco SM-X Layer 2/3 ESM allows you to recover from a lost password. The password recovery disable feature allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted.

PREREQUISITES

This recovery procedure requires you have physical access to the service module.

SUMMARY STEPS

1. **hw-module subslot** *slot/bay* **error-recovery** *password_reset*
2. **flash_init**
3. **rename flash:vlan.dat.renamed flash:vlan.dat**
4. **delete flash:config.text.renamed**

5. **delete flash:private-config.text.renamed**
6. **delete flash:express_setup.debug**
7. **rename flash:config.text flash:config.text.old**
8. **hw-module subslot** *slot/bay* **reload force**
9. **copy flash:**
10. **configure terminal**
11. **enable secret** *password*
12. **exit**
13. **copy running-configuration startup-configuration**
14. **hw-module subslot** *slot/bay* **reload force**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**hw-module** *subslot slot/bay* **error-recovery** *password_reset* **Example:** `Router# hw-module subslot1/0 error-recovery password_reset`	Initiates password recovery process.
Step 2	**flash_init** **Example:** `switch: flash_init`	Initializes the flash memory file system.
Step 3	**rename filesystem:/source-file-url filesystem:/destination-file-url** **Example:** `switch: rename flash:vlan.dat.renamed flash:vlan.dat`	Renames the "vlan.dat.renamed" file to "vlan.dat"
Step 4	**delete filesystem:/file-url** .. **Example:** `switch: delete flash:config.text.renamed`	Deletes the file from the specified file system,
Step 5	**delete flash:** *filename* **Example:** `switch: delete flash:private-config.text.renamed`	Deletes the "**private-config.text.renamed**" file created by the **express_setup** process which was triggered by the execution on the **password_reset** command.
Step 6	**delete flash:** *filename* **Example:** `switch: delete flash:express_setup.debug`	Deletes the express_setup.debug file created by the express_setup.
Step 7	**rename filesystem:/source-file-url filesystem:/destination-file-url** **Example:** `switch: rename flash:config.text flash:config.text.old`	Renames the configuration file to config.text.old.
Step 8	**hw-module subslot** ***slot/bay*** **reload force** **Example:** `hw-module subslot 1/0 reload force`	Use the router hw-module reload force command to reload switch module.

	Command or Action	Purpose
Step 9	**copy flash:** **Example:** `Switch# copy flash:config.text system:running-config`	Copies the configuration file into memory.
Step 10	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 11	**enable secret** *password* **Example:** `Switch(config)# enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0`	Sets the password. • The secret password can be from 1 to 25 alphanumeric characters. • It can start with a number. • It is case sensitive. • It allows spaces but ignores leading spaces.
Step 12	**exit** **Example:** `switch(config)# exit`	Returns you to privileged EXEC mode.
Step 13	**copy running-configuration startup-configuration** **Example:** `switch# copy running-config startup-config`	Copies the configuration from the running configuration file to the switch startup configuration file. • This procedure is likely to leave your Cisco enhanced EtherSwitch service module virtual interface in a shut down state. • You can see which interface is in this state by entering the **show running-configuration** privileged EXEC command. • To reenable the interface, enter the **interface vlan** *vlan-id* global configuration command, and specify the VLAN ID of the shut down interface. With the Cisco enhanced EtherSwitch service module in interface configuration mode, enter the **no shutdown** command.
Step 14	**hw-module subslot** *slot/bay* **reload force** **Example:** `Router# hw-module subslot 1/0 reload force`	Reloads and restarts the ESM. The “force” option allows you to proceed without prompting you for confirmation.

Example

Sample Output for Recovering from a Lost or Forgotten Password

```
Router# hw-module subslot 1/0 error-recovery password_reset
Router# hw-module session 1/0
The password-recovery mechanism is enabled.
The system has been interrupted prior to initializing the flash filesystem.  The following
commands will initialize the flash filesystem, and finish loading the operating system
software:

  flash_init
    boot
  switch:
  switch:
 Router# hw-module subslot 1/0 reload force
```

Related Documentation

Related Topic	Document Title
Hardware installation instructions for network modules	*Connecting Cisco SM-X Layer 2/3 EtherSwitch Service Module to the Network*
General information about configuration and command reference.	*Software Configuration Guide for the Cisco 4451-X Integrated Services Router*
Regulatory compliance information for Cisco 4451-X ISR.	*Regulatory Compliance and Safety Information for the Cisco 4451-X Integrated Services Router*
Boot Loader Command Reference.	*Catalyst 3750 Switch Bootloader Commands*
Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2	*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*
Catalyst 3750-X and 3560-X Switch Software Configuration Guide	*Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE*

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

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