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

April 2, 2014

The Cisco SM-X Layer 2/3 EtherSwitch Service Modules (Cisco SM-X Layer 2/3 ESM) integrates the Layer 2 and Layer 3 switching features and provide the Cisco 2900 series and Cisco 3900 series ISRs 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) that work on multiple router families

The Cisco SM-X Layer 2/3 ESM can co-exist with EtherSwitch service modules from previous releases on the host Cisco 2900 and 3900 series ISRs and these modules are capable of interoperability with each other. Support for the maximum number of service modules that can be present on the 2900 and 3900 series ISRs is dictated by the total number of service module slot count on the host router.

The following are the feature histories for the Cisco SM-X Layer 2/3 ESMs:

Cisco Systems, Inc.
www.cisco.com

Table 1 *Feature History for Cisco SM-X Layer 2/3 ESM (SM-X-ES3-16-P, SM-X-ES3-24-P, and SM-X-ES3D-48-P)*

Release	Modification
Cisco IOS Release15.3(3)M (router software) Cisco IOS Release 15.0(2)EJ (switch software)	Modified for Layer 3 switches
Cisco IOS Release 15.4(1) T (router software) Cisco IOS Release 15.0(2)EJ1 (switch software)	Support for SM-X-ES3D-48-P was added.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Prerequisites for the Cisco SM-X Layer 2/3 ESMs

The Cisco IOS version on the Cisco SM-X Layer 2/3 ESMs must be compatible with the Cisco IOS software release and feature set on the router. See the Feature History for Cisco SM-X Layer 2/3 ESM (SM-X-ES3-16-P, SM-X-ES3-24-P, and SM-X-ES3D-48-P).

- To view the router, 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 version, enter the **service-module gigabitethernet x/0 status** command in privileged EXEC mode, where X is the slot number.

Information About the Cisco SM-X Layer 2/3 ESMs

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

- Hardware Overview, page 3
- Software Features, page 3
- Maximum Number of Modules Supported on Each Platform

- Managing Cisco SM-X Layer 2/3 ESM Using Cisco IOS Software, page 6

Note For a list of Switch IOS feature documentation with information on various supported features on your Cisco SM-X Layer 2/3 ESM, see the Related Documents, page 32

Maximum Number of Modules Supported on Each Platform

Table 2 shows number of modules supported on each Cisco ISR-G2 platform.

Table 2 Maximum number of modules supported per Cisco ISR-G2 router

Modules	Cisco 2911	Cisco 2921	Cisco 2951	Cisco 3925	Cisco 3925 E	Cisco 3945	Cisco 3945 E
SM-X-ES3-16-P	1	1	2	2	2	4	4
SM-X-ES3-24-P	1	1	2	2	2	4	4
SM-X-ES3D-48-P	0	1	1	1	1	1	1

Note The number value in Table 2 indicates the maximum number of Cisco SM-X Layer 2/3 ESMs supported on each router when no other SMs are present on the router.

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 ESMs can be deployed as backbone switches, aggregating 10BASE-T, 100BASE-T, and 1000BASE-T Ethernet traffic from other network devices.

The following Cisco SM-X Layer 2/3 ESMs are available with this release of the hardware:

- SM-X-ES3-16-P—16-port 10/100/1000 Gigabit Ethernet, PoE+, MACSec enabled Service Module, single-wide form factor
- SM-X-ES3-24-P—24-port 10/100/1000 Gigabit Ethernet, PoE+, MACSec 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 new features supported in 15.3(3)M release:

Cisco Trust Sec 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* for information on configuring this feature.

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 highest level of license 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.

You can deploy a specific feature package by applying corresponding software activation licenses. 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 encyprtion 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 (PD) 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+), that increases the available power for PDs from 15.4W 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 through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power Cisco PDs to operate at its highest power mode.

The PoE plus feature enable 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)

The power policing or power sensing feature allows you 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 *Power Monitoring and Power Policing* section in the *Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later*

Smart Install Support

The Cisco SM-X Layer 2/3 ESM supports the Smart Install feature. The Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. You can ship a switch to a location, place it in the network and power it on with no configuration required on the device.

A network using Smart Install includes a group of networking devices, known as clients, that are served by a common Layer 3 switch or router that acts as a director. In a Smart Install network, you can use the Zero-Touch Installation process to install new access layer switches into the network without any assistance from the network administrator. The *Smart Install Configuration Guide* provides detailed information on configuring and using this feature.

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

This sections contains the following topics with information on configuring and managing the Cisco SM-X Layer 2/3 ESM on Cisco ISR-G2 using the Cisco IOS software:

- Using OIR to Manage the Cisco SM-X Layer 2/3 ESM, page 6
- Managing Backplane Switch Ports, page 6
- Internal Port Mapping, page 7

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 router. The Cisco SM-X Layer 2/3 ESM must be gracefully powered down before removing it from the router using the managed OIR or soft OIR feature. The managed OIR feature allows you to stop the power supply to your module using the **hw-module sm** command and remove a 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 **oir-stop** option allows you to gracefully deactivate a module and the module is rebooted when the- **oir-start** option of the command is executed. The reload option will stop or deactivate a specified module and restart it. See the Shutting Down, Resetting, and Reloading the Cisco SM-X Layer 2/3 ESM for more information.

Note The managed OIR feature is only supported on Cisco 3900 Series ISR.

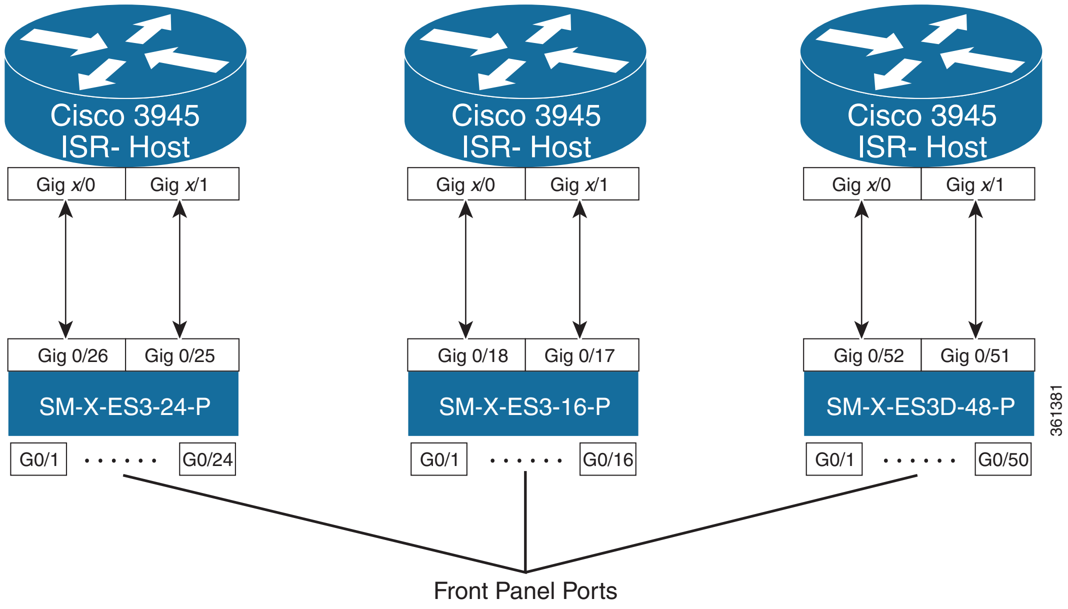
Managing Backplane Switch Ports

When there are no legacy switch modules such as the HWIC-4ESW module in the router, a 2nd GE **interface gigabitethernet** *slot/1* is created for the SM. This is a Layer-2 switch interface and used to manage the inter module connectivity with other SM in the system via the backplane MGF. You can use the switchport CLIs to manage the L2 switch properties (e.g. access mode, trunk mode, native vlan etc.) for this interface. See the,“Maximum Number of Modules Supported on Each Platform” section on page 3 to view a list of modules supported on each platform.

Internal Port Mapping

The Figure 1 below displays the internal port mapping for the Cisco SM-X Layer 2/3 ESM for the Cisco ISR G2. The variable "x" indicates the slot number where the Cisco SM-X-ES3-24-P, Cisco SM-X-ES3-16-P, and the SM-X-ES3D-48-P SKUs of the module are inserted on Cisco 3945 ISR G2.

Figure 1 Port Mapping for Cisco SM-X Layer 2/3 ESM on Cisco ISR G2



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

This section contains the following procedures:

- Accessing the CLI Through a Console Connection or Through Telnet, page 7 (required)
- Configuring the Cisco SM-X Layer 2/3 ESM in the Router, page 8
- Module-to-Module Communication, page 23
- Monitoring Real-Time Power Consumption (power sensing), page 15
- Shutting Down, Resetting, and Reloading the Cisco SM-X Layer 2/3 ESM, page 14
- Understanding Interface Types on the Cisco SM-X Layer 2/3 ESMs, page 8 (optional)

Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the Cisco SM-X Layer 2/3 ESM CLI, you must connect to the host router through the router console or through Telnet. Once you are connected to the router, you must configure an IP address on the Gigabit Ethernet interface connected to the Cisco SM-X Layer 2/3 ESM. Open a session to the Cisco SM-X Layer 2/3 ESM using the **service-module** *gigabitethernet x/0* **session** command in privileged EXEC mode on the router.

You can use one of these methods to establish a connection to the Cisco SM-X Layer 2/3 ESM:

- Connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **service-module** *gigabitethernet x/0* **session** command in privileged EXEC mode on the router.

  Note When connecting to the router through the console using Telnet or SSH from a client station, you must have IP connectivity from the station to the switch.

Note The default baud rate of the console connection is 9600.

- Use any Telnet TCP/IP or encrypted SSH package from a remote management station. The internal interface must have network connectivity with the Telnet or SSH client, and the internal interface must have an enable secret password configured. After you connect through the CLI, a Telnet session, or an SSH session, the user EXEC prompt appears on the management station.

  The Cisco SM-X Layer 2/3 ESM or switch supports up to 5 simultaneous secure SSH sessions and up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

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

- To configure an IP address and subnet mask for Gigabit Ethernet interface (gigabitethernet 1/0) on the router, use the following command:

```
Router(config)#interface gigabitethernet 1/0
Router(config-if)#ip address 10.1.1.111 255.255.255.252
Router(config-if)#no shutdown
```

- To open a session from the router to the Cisco SM-X Layer 2/3 ESM, use the following command:

```
Router#service-module gigabitethernet1/0 session
```

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

This section describes the different types of interfaces supported by the Cisco SM-X Layer 2/3 ESM with references to chapters that contain more detailed information about configuring these interface types.

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

- Gigabit Ethernet interfaces
- VLAN switched virtual interface (SVI)

Configuring the Cisco SM-X Layer 2/3 ESM in the Router

This section describes how to perform the initial configuration on the router with a Cisco SM-X Layer 2/3 ESM installed. This section also describes the initial configuration on the Cisco SM-X Layer 2/3 ESM itself. Once an IP address has been configured on the Gigabit Ethernet interface on the router (representing the Cisco SM-X Layer 2/3 ESM), you can open a console session to the Cisco SM-X Layer 2/3 ESM and configure its Gigabit Ethernet interface for Layer 2 or Layer 3 features.

Once the Cisco SM-X Layer 2/3 ESM interface has been configured and you boot up the service module image, you can switch back and forth between the router and the service module.

Note 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 boot manually or, if a corrupted Cisco IOS image is loaded. You can also access the boot loader if you have lost or forgotten the switch password.

Note Step 9 and 10 are not required in releases prior to Release 15.5(03)M06.

SUMMARY STEPS

1. **dir flash:**
2. **boot flash:***image-name*
3. **enable**
4. **show running interface**
5. **configure terminal**
6. **interface gigabitethernet** *slot/port*
7. **ip address** *ip address/subnet mask*
8. **no shutdown**
9. **line** *tty line number*
10. **transport input all**
11. **end**
12. **service-module** *interface slot/port* ***session***
13. **enable**
14. **show ip interface brief**
15. **control+shift+6 x**
16. **disconnect**
17. **service-module gigabitethernet** *slot/port* **status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dir flash**: **Example:** `rommon> dir flash:`	Displays a list of all files and directories in router flash memory.
Step 2	**boot flash**:*image-name* **Example:** `rommon> boot flash:c3900-universalk9-mz`	Boots the router image that supports the Cisco SM-X Layer 2/3 ESM. • Enter **no** when prompted to enter the initial configuration dialog and then press **Enter**.
Step 3	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode.
Step 4	**show running interface** **Example:** `Router# show running interface gigabitethernet1/0`	Displays the running interface of the router, which should have a Gigabit Ethernet interface representing the Cisco SM-X Layer 2/3 ESM.
Step 5	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 6	**interface gigabitethernet** *slot/port* **Example:** `Router(config)# interface gigabitethernet1/0`	Enters interface configuration mode and specifies an interface for configuration.
Step 7	**ip address** *ip address/subnet mask* **Example:** `Router(config-if)# ip address 20.0.0.1 255.255.255.0`	Configures an IP address and subnet mask on this Gigabit Ethernet interface.
Step 8	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the service module port.

	Command or Action	Purpose
Step 9	**line** *tty line number* **Example:** `Router(config)# line 67`	Identifies a specific line for configuration and enters the line configuration collection mode. **Note** TTY Line number varies based on the module inserted on the slot. **Note** This step is not required in releases prior to Release 15.5(03)M06.
Step 10	**transport input all** **Example:** `Router(config)# transport input all`	Assigns the device or interface as the designated-gateway for the domain. **Note** This step is not required in releases prior to Release 15.5(03)M06.

Step 11	**end**
	Example:
	`Router(config-if)# end`
		Returns you to privileged EXEC mode.

Step 12	**service-module** *interface slot/port* **session** **Example:** `Router# service-module gigabitethernet1/0 session`	Connects to and opens a session on the Cisco SM-X Layer 2/3 ESM.
Step 13	**enable** **Example:** `Switch> enable`	Enters privileged EXEC mode on the Cisco SM-X Layer 2/3 ESM.
Step 14	**show ip interface brief** **Example:** `Switch# show ip interface brief`	Displays brief version of the Cisco SM-X Layer 2/3 ESM configuration information.
Step 15	**control+shift+6 x** **Example:** `Switch#` **control+shift+6 x**	Returns you to the router console while keeping the console session to the switch intact.

	Command or Action	Purpose
Step 16	**disconnect** **Example:** `Router# disconnect`	Terminates the console session to the Cisco SM-X Layer 2/3 ESM.
Step 17	**service-module gigabitethernet** *slot/port* **status** **Example:** `Router# service-module gigabitethernet 1/0 status`	Displays the service module status information.

Examples

The sections provides the following example:

Sample Uutput From the show version Command

The following example displays the configuration details of the Cisco SM-X Layer 2/3 ESM configured on the router.

```
Switch# show version
Cisco IOS Software, C3560E Software (C3560E-UNIVERSALK9-M), Version 15.0(2)EJ, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 12:09 by prod_rel_team

ROM: Bootstrap program is C3560E boot loader
BOOTLDR: C3560E Boot Loader (C3560X-HBOOT-M) Version 15.0(2r)EJ, RELEASE SOFTWARE (fc1)

Switch uptime is 1 hour, 55 minutes
System returned to ROM by power-on
System restarted at 06:49:50 UTC Wed Nov 13 2013
System image file is "flash:c3560e-universalk9-mz.150-2.EJ"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: ipservices
License Type: Permanent Right-To-Use
Next reload license Level: ipservices

cisco SM-X-ES3-16-P (PowerPC405) processor with 262144K bytes of memory.
Processor board ID FOC17223S3Z
Last reset from power-on
1 Virtual Ethernet interface
18 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : EC:E1:A9:5A:C3:00
Model number                    : SM-X-ES3-16-P
System serial number            : FOC17223S3Z
Hardware Board Revision Number  : 0x00


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 18    SM-X-ES3-16-P      15.0(2)EJ             C3560E-UNIVERSALK9-M


Configuration register is 0xF

Switch#
```

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

This section describes how to shut down, reset, and reload a Cisco SM-X Layer 2/3 ESM after it has been installed.

SUMMARY STEPS

1. **service-module gigabitethernet** *slot/port* **shutdown**
2. **service-module gigabitethernet** *slot/port* **reset**
3. **service-module gigabitethernet** *slot/port* **reload**

Note The argument ***slot*** indicates the number of the router chassis slot for the service module. The argument ***unit*** indicates the number of the daughter card on the service module. For Cisco SM-X Layer 2/3 ESMs, always use 0.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**service-module gigabitethernet** *slot/port* **shutdown** **Example:** `Router# service-module gigabitethernet1/0 shutdown`	Performs a graceful halt of the Cisco SM-X Layer 2/3 ESM operating system. Use the **service-module reset** command to power up the service module again. **Note** Use the **hw-module** *slot / port* **oir-stop** command when removing or replacing a hot-swappableCisco SM-X Layer 2/3 ESM during online insertion and removal (OIR).
Step 2	**service-module gigabitethernet** *slot/port* **reset** **Example:** `Router# service-module gigabitethernet1/0 reset`	Performs a hardware reset of the Cisco SM-X Layer 2/3 ESM.
Step 3	**service-module gigabitethernet** *slot/port* **reload** **Example:** `Router# service-module gigabitethernet1/0 reload`	Performs a graceful halt and reload of the Cisco SM-X Layer 2/3 ESM operating system. The configuration of the switch is saved before reload.

Examples

This section provides the following examples:

- Sample Output for the service-module gigabitethernet shutdown Command, page 14
- Sample Output for the service-module gigabitethernet reset Command, page 15
- Sample Output for the service-module gigabitethernet reload Command, page 15

Sample Output for the service-module gigabitethernet shutdown Command

The following example shows what appears when you enter the **service-module gigabitethernet** *slot/port* **shutdown** command:

```
Router# service-module gigabitethernet1/0 shutdown
```

```
Shutdown is used for Online removal of Service Module.
Do you want to proceed with shutdown?[confirm]
Use service-module reset command to recover from shutdown.
```

Note At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Sample Output for the service-module gigabitethernet reset Command

The following example shows what appears when you enter the **service-module gigabitethernet** *slot/port* **reset** command:

```
Router# service-module g3/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the NVRAM, nonvolatile file system or unsaved configuration!
Do you want to reset?[confirm]
```

Note At the confirmation prompt, press **Enter** to confirm the action or **n** to cancel.

Sample Output for the service-module gigabitethernet reload Command

The following example shows what appears when you enter the **service-module gigabitethernet** *slot/port* **reload** command:

```
Router# service-module gigabitethernet1/0 reload
Do you want to proceed with reload?[confirm]
```

Note At 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 (config-if)** 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 **show power inline** CLI.

You can monitor the power drawn at the router level through **show power inline** command on the Cisco ISR-G2 routers. To monitor port-level power consumption use the **show power inline** command on the Cisco SM-X Layer 2/3 ESM in Exec mode.

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. **interface gigabiethernet** *0/x*
2. **power inline max** *max-wattage*
3. **power inline police action** *action*
4. **exit**

Detailed Steps

	Command or Action	Purpose

Step 1	**`enable`**
	Example:
	`Switch> enable`
		Enters privileged EXEC mode.

Step 2	**`configure terminal`**
	Example:
	`Switch# configure terminal`
		Enters global configuration mode.

Step 3	**`interface gigabitethernet`** *`0/x`*
	Example:
	`Switch(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:
	`Switch(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:
	`Switch(config-if)# power inline police action` *`action`*
		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:
	`Switch(config-if)# exit`
		Exits the interface configuration mode.

Example

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

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
- 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`**
	Example:
	`Switch> enable`
		Enters privileged EXEC mode.

Step 2	**`configure terminal`**
	Example:
	`Switch# configure terminal`
		Enters global configuration mode.

Step 3	**`interface gigabitethernet`** *`0/x`*
	Example:
	`Switch(config)# interface gigabitethernet 0/24`
		Enter interface configuration mode and places you at the GigabitEthernet 0/24 interface.

Step 4	**`no switchport`**
	Example:
	`Switch(config-if)# no switchport`
		Enables the routed port.
		Note The **no switchport** command is only available on the SM-X Layer3 ESMs.

Step 5	**`ip address`** *`ip address/subnet mask 192.1.10.200 255.255.255.240`*
	Example:
	`Switch(config-if)# ip address 192.1.10.200 255.255.255.240`
		Sets a primary or secondary IP address for this interface.

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

	Command or Action	Purpose

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

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 tftpserver 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.

Summary Steps

1. **copy tftp: flash:**
2. **config terminal**
3. **tftp-server flash:** *switch-image*
4. **interface gigabitethernet** *slot/port*
5. **ip address** *ip address/subnet mask*
6. **no shutdown**
7. **end**
8. **service-module gigabitethernet** *slot/port* **session**
9. **config terminal**
10. **interface gigabitethernet** *slot/port*
11. **ip address** *ip address/subnet mask*
12. **copy tftp: flash:**

Detailed Steps

	Command or Action	Purpose

Step 1	**`copy tftp: flash:`**
	Example:
	`Router# copy tftp: flash:`
		Copies an image from a TFTP server to flash memory.

Step 2	**`config terminal`**
	Example:
	`Router# conf t`
		Enters global configuration mode.

Step 3	**`tftp-server flash:`** *`filename`*
	Example:
	`Router(config)#tftp-server flash:c3560e-universalk9-mz`
		Specifies TFTP service of a file on a Flash memory device. Specify the Switch image in the filename parameter.

Step 4	**`interface gigabitethernet`** `x/0`
	Example:
	`Router(config)#interface gigabitethernet1/0`
		Enter interface configuration mode and places you at the GigabitEthernet 0/24 interface.

Step 5	**ip address** *`ip-address subnet-mask`* **Example:** `Router(config-if)#ip address 1.1.1.1 255.255.255.0`	Sets a primary or secondary IP address for this interface.

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

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

Step 8	**`service-module gigabitethernet`** `x/0` **`session`**
	Example:
	`Router# service-module gigabitethernet 1/0 session`
		Connects to the service module and opens a service module session.

Step 9	**`config terminal`**
	Example:
	`Switch#config terminal`
		Enters global configuration mode.

Step 10	**`interface gigabiethernet`** `0/26`
	Example:
	`Switch(config)#interface gigabitether 0/26`
		Enters interface configuration mode and specifies an interface for configuration.

	Command or Action	Purpose
Step 11	**ip address** *ip-address/subnet-mask* **Example:** `Switch(config-if)#ip address 1.1.1.2 255.255.255.0`	Sets a primary or secondary IP address for this interface. **Note** IP address here should in the same subnet as mentioned in the example in Step 5.
Step 12	**no shutdown** **Example:** `Switch(config-if)#no shutdown`	Enables the port that is connected to the TFTP server. **Note** You can skip Steps 4 through 6 and 9 through 11, if there is already reachability between host router and switch module.

Step 13	**end**
	Example:
	`Switch(config-if)#end`
		Exits interface configuration mode, and returns to privileged EXEC mode.

Step 14	**copy tftp: flash:** **Example:** `Switch# copy tftp: flash:`	Copies an image from a TFTP server to flash memory **Note** The tftp server should be 1.1.1.1 or any other reachable ip address from host.

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 **GigabitEthernet X/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 gigabitethernet 1/1
 switchport access vlan 10
!
interface gigabitethernet 2/1
 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 SM-X Layer 2/3 ESM:

- Recovering from a Corrupted Software Image Using Recovery Image, page 24
- Recovering from a Lost or Forgotten Password, page 25
- Recovering from a Lost or Forgotten Password When Password Recovery Is Disabled, page 27

Recovering from a Corrupted Software Image Using Recovery Image

This section describes how to recover from a corrupted software image by using a recovery image.

Note The router should have the switch image in the router flash memory or have network connectivity to the TFTP server.

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** CLI 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 ESM is booted, desired Cisco.com switch image can be copied to the ESM 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 ESM 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 17.

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 an end user 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 ESMs allows an end user 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, the user 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 to have physical access to the service module.

SUMMARY STEPS

1. **service-module** *interface slot/port* **password-reset**
2. **flash_init**
3. **rename**
4. **boot**
5. **copy flash:**
6. **configure terminal**
7. **enable secret** *password*
8. **exit**
9. **copy running-configuration startup-configuration**
10. **reload**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**service-module** *interface slot/port* **password-reset** **Example:** `Router# service-module gigabitethernet1/0 password-reset`	Enables password recovery.
Step 2	**flash_init** **Example:** `switch: flash_init`	Initializes the flash memory file system.
Step 3	**rename** **Example:** `switch: rename flash:config.text flash:config.text.old`	Renames the configuration file to config.text.old.
Step 4	**boot [-x] [-v] [device:][imagename]** **Example:** `switch: boot`	Use the boot command to boot up an external process.
Step 5	**copy flash:** **Example:** `Switch# copy flash:config.text system:running-config`	Copies the configuration file into memory.
Step 6	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 7	**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 8	**exit** **Example:** `Switch(config)# exit`	Returns you to privileged EXEC mode.

	Command or Action	Purpose
Step 9	**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 SM-X Layer 2/3 ESM 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 re-enable the interface, enter the **interface vlan** *vlan-id* global configuration command, and specify the VLAN ID of the shut down interface. With the Cisco SM-X Layer 2/3 ESM in interface configuration mode, enter the **no shutdown** command.
Step 10	**reload** **Example:** `Switch# reload`	Reloads the switch.

Recovering from a Lost or Forgotten Password When Password Recovery Is Disabled

When password recovery is disabled, access to the boot loader prompt through the password-recovery mechanism is disallowed even though the password-recovery mechanism has been triggered. If you agree to let the system be reset to the default system configuration, access to the boot loader prompt is then allowed, and you can set the environment variables.

SUMMARY STEPS

1. **service-module** *interface slot/port* **password-reset**
2. **service-module** *interface slot/port* **session**
3. **dir flash:**
4. **boot**
5. **enable**
6. **configure terminal**
7. **enable secret** *password*
8. **exit**
9. **copy running-configuration startup-configuration**
10. **reload**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`service-module`** *`interface slot/port`* **`password-reset`**
	Example:
	`Router# service-module gigabitethernet1/0 password-reset`
		Resets the password on the router.

Step 2	**`service-module`** *`interface slot/port`* **`session`**
	Example:
	`Router# service-module gigabitethernet 1/0 session`
		Connects to the service module and opens a service module session.
		• Entering **no** leaves the current configuration file intact, so you can rename it.
		• Entering **yes** deletes the configuration file.
		Note This configuration can only be done if the **service-module session** command is entered within 50 seconds after entering the **service-module password-reset** command.

Step 3	**`dir flash:`**
	Example:
	`switch: dir flash:`
		Displays a list of all files and directories in flash memory on the service module.

Step 4	**`boot`**
	Example:
	`switch: boot`
		Boots the system.

Step 5	**`enable`**
	Example:
	`Switch> enable`
		Enters privileged EXEC mode from the service module prompt.

Step 6	**`configure terminal`**
	Example:
	`Switch# configure terminal`
		Enters global configuration mode.

Step 7	**`enable secret`** *`password`*
	Example:
	`Switch(config)# enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0`
		Changes 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 8	**`exit`**
	Example:
	`Switch(config)# exit`
		Returns you to privileged EXEC mode.

	Command or Action	Purpose

Step 9	`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 SM-X Layer 2/3 ESM 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 SM-X Layer 2/3 ESM in interface configuration mode, enter the **no shutdown** command.

Step 10	`reload`
	Example:
	`Switch# reload`
		Reloads the switch.
		Note This does not set the environment variables if the switch is set to auto boot.

Example

Sample Output for Recovering from a Lost or Forgotten Password When Password Recovery is Disabled

```
Switch#conf t
Switch(config)#no service password-recovery
Switch(config)#end
Switch#
c3945#disconnect
Closing connection to 99.0.0.1 [confirm]
c3945#
c3945#service-module gig4/0 password-reset
Do you want to proceed with password reset process?[confirm]
Starting password reset process...
Wait for 50 secs for password reset process to complete
c3945#
c3945#
*Nov 13 10:17:36.488 IST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet4/1, changed state to down
c3945#service-module gig4/0 sess
Trying 99.0.0.1, 2259 ... Open

Using driver version 3 for media type 2
Base ethernet MAC Address: 04:da:d2:ef:a0:00
Xmodem file system is available.
The password-recovery mechanism is disabled.


Password reset process is complete...

Initializing Flash...
mifs[2]: 12 files, 1 directories
mifs[2]: Total bytes     :    2097152
mifs[2]: Bytes used      :     888832
mifs[2]: Bytes available :    1208320
mifs[2]: mifs fsck took 1 seconds.
mifs[3]: 1 files, 1 directories
mifs[3]: Total bytes     :    4194304
mifs[3]: Bytes used      :     217088
mifs[3]: Bytes available :    3977216
mifs[3]: mifs fsck took 1 seconds.
mifs[4]: 5 files, 1 directories
mifs[4]: Total bytes     :     524288
mifs[4]: Bytes used      :      49152
mifs[4]: Bytes available :     475136
mifs[4]: mifs fsck took 1 seconds.
mifs[5]: 5 files, 1 directories
mifs[5]: Total bytes     :     524288
mifs[5]: Bytes used      :      49152
mifs[5]: Bytes available :     475136
mifs[5]: mifs fsck took 0 seconds.
mifs[6]: 1 files, 1 directories
mifs[6]: Total bytes     :   30408704
mifs[6]: Bytes used      :   20324352
mifs[6]: Bytes available :   10084352
mifs[6]: mifs fsck took 8 seconds.
mifs[7]: 8 files, 1 directories
mifs[7]: Total bytes     :   88735744
mifs[7]: Bytes used      :   63512576
mifs[7]: Bytes available :   25223168
mifs[7]: mifs fsck took 24 seconds.
...done Initializing Flash.
```

```
done.
Verifying image ucode0:usbdos.dl....
Image passed digital signature verification
Verifying bootloader image........
BootLoader self verification passed


The password-recovery mechanism has been triggered, but
is currently disabled.  Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point.  However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?y


The system has been interrupted, and the config file
has been deleted.  The following command will finish
loading the operating system software:

    boot


switch: boot
Loading "flash:c3560e-universalk9-mz"...Verifying image flash:c3560e-universalk9-mz

<omitted non relevant boot logs>


         --- System Configuration Dialog ---

Enable secret warning
----------------------------------
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the intial configuration dialog, or if you exit setup without
setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
----------------------------------
Would you like to enter the initial configuration dialog? [yes/no]:
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
Switch>
Nov 13 04:53:57.888: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively
down
Nov 13 04:53:57.896: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to down
Switch>
```

Related Documents

Related Topic	Document Title
Hardware installation instructions for network modules	*Cisco 2900 Series and 3900 Series Hardware Installation*
General information about configuration and command reference.	*Cisco 3900 Series, 2900 Series, and 1900 Series Integrated Services Routers Software Configuration Guide*
General information about configuring all supported Switching features.	*Catalyst 3560 Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later*
Configurationg information about Cisco Enhanced EtherSwitch Service Modules support on ISR G2	*Cisco Enhanced EtherSwitch Service Modules Configuration Guide*
Regulatory compliance information for Cisco 2900 series routers.	*Regulatory Compliance and Safety Information for Cisco 2900 Series Integrated Services Routers*
Regulatory compliance information for Cisco 3900 series routers.	*Regulatory Compliance and Safety Information for Cisco 3900 Series Integrated Services Routers*

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.