Cisco Enhanced EtherSwitch Service Modules Configuration Guide

The Cisco enhanced EtherSwitch service modules provide Cisco 2900 series routers and Cisco 3900 series routers the ability to use Cisco enhanced EtherSwitch service modules as independent Layer 2 and Layer 3 switches when running Cisco IOS.

Note This document describes the following Cisco enhanced EtherSwitch service modules only: SM-ES2-16-P, SM-ES3-16-P, SM-ES3G-16-P, SM-ES2-24, SM-ES2-24-P, SM-ES3-24-P, SM-ES3G-24-P, SM-D-ES2-48, SM-D-ES3-48-P, and SM-D-ES3G-48-P. For information about other Cisco Ethernet switch network modules, see the Connecting Cisco Ethernet Switch Network Modules to the Network document.

The Cisco enhanced EtherSwitch service modules connect to Cisco 2900 series and Cisco 3900 series routers through the service module console Gigabit Ethernet port to a serial interface on the router. This Gigabit Ethernet port gives the appearance of a Layer 3 port to the router.

The Cisco enhanced EtherSwitch service modules also provide a physical Gigabit Ethernet serializer/deserializer integrated circuit transceiver High-Speed Intrachassis Module Interconnect (HIMI) interface. In the Cisco 2900 series and Cisco 3900 series routers, the HIMI link on the Cisco enhanced EtherSwitch service modules is connected to the router internal Gigabit Ethernet backplane. This link is used for interconnection between other interface cards or network modules attached to the router Gigabit Ethernet backplane bypassing the router host CPU, thus increasing CPU performance by decreasing CPU processing.

To access the Cisco enhanced EtherSwitch service module, establish a session from the router over the serial interface to the Cisco enhanced EtherSwitch service module. To exchange and monitor control messages between the Cisco enhanced EtherSwitch service module and the router, a Router Blade Configuration Protocol (RBCP) stack operates concurrently on active IOS sessions running on both the router and the service module.

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

Feature History for the Cisco Enhanced EtherSwitch Service Modules (SM-ES2-16-P, SM-ES3-16-P, SM-ES3G-16-P, SM-ES2-24, SM-ES2-24-P, SM-ES3-24-P, SM-ES3G-24-P, SM-D-ES2-48, SM-D-ES3-48-P, and SM-D-ES3G-48-P)

Release	Modification
12.2(52)EX (switch software)	This feature was introduced.
15.0(1)M (router software)	This feature was introduced.

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 Enhanced EtherSwitch Service Modules

The Cisco IOS version on the Cisco enhanced EtherSwitch service modules must be compatible with the Cisco IOS software release and feature set on the router. See the "Feature History for the Cisco Enhanced EtherSwitch Service Modules (SM-ES2-16-P, SM-ES3-16-P, SM-ES3G-16-P, SM-ES2-24, SM-ES2-24-P, SM-ES3-24-P, SM-ES3G-24-P, SM-D-ES2-48, SM-D-ES3-48-P, and SM-D-ES3G-48-P)" section on page 2.

- To view the router, Cisco IOS software release, and feature set, enter the **service module interface status** command in privileged EXEC mode.
- To view the Cisco enhanced EtherSwitch service module IOS version, enter the **show version** command in privileged EXEC mode.

Information About the Cisco Enhanced EtherSwitch Service Modules

This section describes the features and some important concepts about the Cisco enhanced EtherSwitch service modules.

Hardware Overview

Cisco enhanced EtherSwitch service modules 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.

Note Cisco enhanced EtherSwitch service module model SM-ES2-24 does not support IP phones.

The Cisco enhanced EtherSwitch service modules can be deployed as backbone switches, aggregating 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet traffic from other network devices.

Note You can install up to one Cisco enhanced EtherSwitch service module in Cisco 2911 routers and in Cisco 2921 routers. You can install up to two Cisco enhanced EtherSwitch service modules in Cisco 2951 and Cisco 3925 routers. You can install up to four Cisco enhanced EtherSwitch service modules in Cisco 3945 routers.

The following Cisco enhanced EtherSwitch service modules are available with this release of the hardware:

- SM-ES2-16-P—15 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, single-wide Layer 2 enhanced EtherSwitch service module, with power over Ethernet (PoE) support
- SM-ES3-16-P—15 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, single-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
- SM-ES3G-16-P—16 10/100/1000 Ethernet port, single-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
- SM-ES2-24—23 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, single-wide Layer 2 enhanced EtherSwitch service module, with no PoE support
- SM-ES2-24-P—23 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, single-wide Layer 2 enhanced EtherSwitch service module, with PoE support
- SM-ES3-24-P—23 10/100 Ethernet ports, 1 10/100/1000 Ethernet port, single-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
- SM-ES3G-24-P—24 10/100/1000 Ethernet port, single-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
- SM-D-ES2-48—48 10/100 Ethernet port, double-wide Layer 2 enhanced EtherSwitch service module
- SM-D-ES3-48-P—48 10/100 Ethernet port, double-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support
- SM-D-ES3G-48-P—48 10/100/1000 Ethernet port, double-wide Layer 2 and Layer 3 enhanced EtherSwitch service module, with PoE support

Note To install double-wide service modules in the Cisco 3900 series routers, remove the slot divider between slots SM3 and SM4 (3945) and remove the blank panel to the right of SM2 (3925).

For complete information about the Cisco enhanced EtherSwitch service modules hardware, see *Connecting Cisco Enhanced EtherSwitch Service Modules to the Network* at the following URL:

http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/eesm_hw.html

How to Configure the Cisco Enhanced EtherSwitch Service Module on the Router

This section contains the following procedures:

Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the Cisco enhanced EtherSwitch service module 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 enhanced EtherSwitch service module. Open a session to the Cisco enhanced EtherSwitch service module 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 enhanced EtherSwitch service module:

- 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.

- 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 enhanced EtherSwitch service module 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
```

- To open a session from the router to the Cisco enhanced EtherSwitch service module, use the following command:

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

Understanding Interface Types on the Cisco Enhanced EtherSwitch Service Modules

This section describes the different types of interfaces supported by the Cisco enhanced EtherSwitch service module with references to chapters that contain more detailed information about configuring these interface types.

The Cisco enhanced EtherSwitch service module supports the following interface types:

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

Using Interface Configuration Mode

You can configure the individual Cisco enhanced EtherSwitch service module physical interfaces (ports) through the interface configuration mode on the CLI.

- Type—Fast Ethernet (fastethernet or fa) for 10/100-Mbps Ethernet or Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000-Mbps Ethernet ports.
- Module number—The module slot number on the Cisco enhanced EtherSwitch service module or switch (always 0 on the service module or switch).
- Port number—The interface number on the Cisco enhanced EtherSwitch service module or switch. The port numbers always begin at 1, starting at the right when facing the front of the Cisco enhanced EtherSwitch service module, for example, gigabitethernet 0/1, gigabitethernet 0/2 with 0/1 on the top, 0/2 on the bottom, 0/3 on the top, 0/4 on the bottom and so on.

You can identify physical interfaces by physically checking the interface location on the Cisco enhanced EtherSwitch service module. 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.

These are examples of specifying interfaces:

- To specify Gigabit Ethernet port 4 on a standalone Cisco enhanced EtherSwitch service module, enter this command in global configuration mode:

```
Enhanced Switching (config)# interface gigabitethernet 0/4
```

Configuring the Cisco Enhanced EtherSwitch Service Module in the Router

This section describes how to perform the initial configuration on the router with a Cisco enhanced EtherSwitch service module installed. This section also describes the initial configuration on the Cisco enhanced EtherSwitch service module itself. Once an IP address has been configured on the Gigabit Ethernet interface on the router (representing the Cisco enhanced EtherSwitch service module), you can open a console session to the Cisco enhanced EtherSwitch service module and configure its Fast Ethernet and Gigabit Ethernet interfaces for Layer 2 or Layer 3 functionality.

Once the Cisco enhanced EtherSwitch service module 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 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 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** *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/unit* **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:c3945sm-lanbasek9-mz`	Boots the router image that supports the Cisco enhanced EtherSwitch service module. • 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 enhanced EtherSwitch service module.
Step 5	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 6	**interface** *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 enhanced EtherSwitch service module.
Step 13	**enable** **Example:** `Switch> enable`	Enters privileged EXEC mode on the Cisco enhanced EtherSwitch service module.
Step 14	**show ip interface brief** **Example:** `Switch# show ip interface brief`	Displays brief version of the Cisco enhanced EtherSwitch service module 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 enhanced EtherSwitch service module.
Step 17	**service-module gigabitethernet** *slot/unit* **status** **Example:** `Router# service-module gigabitethernet 1/0 status`	Displays the PoE statistics maintained on the Cisco enhanced EtherSwitch service module from the router. **Note** PoE statistics are updated dynamically. **Note** To view PoE statistics on the EtherSwitch module, use the **show power inline** command.

Examples

This section provides the following examples:

Sample Output for the dir flash: Command on the Router

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

```
Router> dir flash:
Directory of flash:/

program load complete, entry point: 0x8000f000, size: 0xc0c0

Initializing ATA monitor library.......
Directory of flash:

2      29823132  -rw- c2960sm-lanbasek9-mz.image
```

Sample Output for the boot flash: Command on the Router

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

```
Router> boot flash:c2960sm-lanbasek9-mz.image
```

```
program load complete, entry point: 0x8000f000, size: 0xc0c0

Initializing ATA monitor library.......

program load complete, entry point: 0x8000f000, size: 0x1c70efc
Self decompressing the image :
################################################################################################
######################################### [OK]
...
```

After the router completes the boot process, you will be prompted to enter the initial configuration dialog as in the following example. Enter **no**.

```
Would you like to enter the initial configuration dialog? [yes/no]: no

Press RETURN to get started!
```

Press **Enter**. You will be at the router prompt.

Sample Output for the show running interface Command on the Router

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

```
Router# show running interface gigabitethernet2/0
Building configuration...

Current configuration : 61 bytes
!
interface GigabitEthernet2/0
 no ip address
 shutdown
end
```

Sample Output for Configuring the Cisco Enhanced EtherSwitch Service Module Interface on the Router

The following example shows an output when you configure the Cisco enhanced EtherSwitch service module on the router:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface GigabitEthernet2/0
Router(config-if)# ip address 20.0.0.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# CNTL/Z
*Jan 10 20:42:08.086: %LINK-3-UPDOWN: Interface GigabitEthernet2/0, changed state to up
*Jan 10 20:42:09.086: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0,
changed state to up
Router(config-if)# end
Router#
```

Sample Output for the service-module Command on the Cisco Enhanced EtherSwitch Service Module

The following example shows what appears when you enter the **service module** command:

```
Router# service-module gigabitethernet2/0 session
Trying 20.0.0.1, 2130 ... Open

Switch:
```

Sample Output for the dir flash: Command on the Cisco Enhanced EtherSwitch Service Module

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

```
Switch: dir flash:
Directory of flash:/

4    -rwx  4814848   <date>              c3560e-universal-image

27698176 bytes available (4815872 bytes used)
Switch:
```

Sample Output for the boot flash: Command on the Cisco Enhanced EtherSwitch Service Module

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

```
Switch: boot flash:c3560e-universal-image
Loading
"flash:c3560e-universal-image"...@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
Switch> end
Switch#
```

Sample Output for the show ip interface brief Command on the Cisco Enhanced EtherSwitch Service Module

The following example shows what appears when you enter the **show ip interface brief** command:

```
Switch# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      unassigned      YES unset  administratively down down
gigabitethernet0/1          unassigned      YES unset  down                  down
gigabitethernet0/2          unassigned      YES unset  down                  down
gigabitethernet0/3          unassigned      YES unset  down                  down
gigabitethernet0/4          unassigned      YES unset  down                  down
gigabitethernet0/5          unassigned      YES unset  down                  down
```

Sample Output for Pressing <Ctrl+Shift+6> Followed by x

The following example shows what appears when you press **<Ctrl+Shift+6>** and then press **x**:

```
Switch# ctrl+shift+6 x
Router#
```

Sample Output for the show power inline Command on the Router

The following example shows what appears when you enter the **show power inline** command on the router:

```
Router# show power inline
PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
INT-PS           0       360.000     0.000         PS1 GOOD   PS2 ABSENT
Interface   Config   Phone    Powered    PowerAllocated
---------   ------   -----    -------    --------------
Gi2/0       auto     Unknown  Off        0.000 Watts
Gi4/0       auto     Unknown  Off        0.000 Watts
Router#
```

Sample Output for the show power inline Command on the Cisco Switching service module

The following example shows what appears when you enter the **show power inline** command on the switch:

```
Switch# show power inline

Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1           360.0        0.0       360.0

Interface  Admin    Oper     Power        Device           Class
                            (Watts)
---------- ----- ---------- ------- ------------------  ----------
gi0/1    auto  off           0.0  n/a                 n/a
gi0/2    auto  off           0.0  n/a                 n/a
gi0/3    auto  off           0.0  n/a                 n/a
gi0/4    auto  off           0.0  n/a                 n/a
gi0/5    auto  off           0.0  n/a                 n/a
gi0/6    auto  off           0.0  n/a                 n/a
gi0/7    auto  off           0.0  n/a                 n/a
-----------------------------------------------------------
```

Shutting Down, Resetting, and Reloading the Cisco Enhanced EtherSwitch Service Module

This section describes how to shut down, reset, and reload a Cisco enhanced EtherSwitch service module after it has been installed.

SUMMARY STEPS

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

Note The argument ***slot*** indicates the number of the router chassis slot for the network module. The argument ***unit*** indicates the number of the daughter card on the network module. For Cisco enhanced EtherSwitch service modules, always use 0.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**service-module gigabitethernet** *slot/unit* **shutdown** **Example:** `Router# service-module gigabitethernet1/0 shutdown`	Performs a graceful halt of the Cisco enhanced EtherSwitch service module operating system. Use the **service-module reset** command to power up the service module again. **Note** Use the **hw-module slot <1-4> oir-stop** command when removing or replacing a hot-swappable Cisco enhanced EtherSwitch service module during online insertion and removal (OIR). **Note** When you shut down the service module using the '**service-module gigabitethernet** *slot/unit* **shutdown**' command, the module prompt will switch to rommon prompt even if the manual boot is configured to 'no'. To bring the module up and running again, run the '**service-module gigabitethernet** *slot/unit* **reset**' command, and then manually boot the module.
Step 2	**service-module gigabitethernet** *slot/unit* **reset** **Example:** `Router# service-module gigabitethernet1/0 reset`	Performs a hardware reset of the Cisco enhanced EtherSwitch service module.
Step 3	**service-module gigabitethernet** *slot/unit* **reload** **Example:** `Router# service-module gigabitethernet1/0 reload`	Performs a graceful halt and reload of the Cisco enhanced EtherSwitch service module 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

The following example shows what appears when you enter the **service-module gigabitethernet *slot/unit* 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/unit* 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/unit* 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.

Upgrading the Cisco Enhanced EtherSwitch Service Module Software

This section describes how to upgrade the Cisco enhanced EtherSwitch service module software by using TFTP.

Restrictions

The procedure in this section is for upgrading a standalone Cisco enhanced EtherSwitch service module in the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *slot/port*
4. **no switchport**
5. **ip address** *ip address/subnet mask*
6. **no shutdown**
7. **end**
8. **show run interface fastethernet**
9. **ping ip address**
10. **show 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** *slot/port* **Example:** `Switch(config)# interface fastethernet 0/24`	Enter interface configuration mode and places you at the Fast Ethernet 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 Layer-3 enhanced EtherSwitch service modules.
Step 5	**ip address** *ip address/subnet mask* **Example:** `Switch(config-if)# ip address 172.16.1.100 255.255.255.0`	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 fastethernet slot/port** **Example:** `Switch# show run interface fastEthernet 0/24`	Shows the configuration applied on this interface.
Step 9	**ping ip address** **Example:** `Switch# ping 172.16.1.100`	Pings for network connectivity.
Step 10	**show flash:** **Example:** `Switch# show flash:`	Displays a list of all files and directories in the Cisco enhanced EtherSwitch service module 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 fastethernet Command, page 19
- Sample Output for the ping tftpserver Command, page 20
- Sample Output for the show flash: Command, page 20
- Sample Output for the copy tftp: flash: Command, page 20

Sample Output for the show run interface fastethernet Command

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

```
Switch# show run interface fa0/24
Building configuration...
Current configuration : 87 bytes
!
interface FastEthernet0/24
 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 **show flash:** command:

```
Switch# show flash:

Directory of flash:/

    3  -rwx     4815232   Jan 1 2009 00:10:53 +00:00 c2960sm-lanbasek9-mz.image
    4  -rwx        6496  May 11 2008 10:43:15 +00:00  vlan.dat
    5  -rwx        2377   Mar 1 2008 04:33:45 +00:00  config.text
    6  -rwx           5   Mar 1 2008 04:33:46 +00:00  private-config.text

15998976 bytes total (6355968 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 []? Tftpserver
Source filename [] c2960sm-lanbasek9-mz
Destination filename [c2960sm-lanbasek9-mz]?
Accessing tftp://tftpserverc2960sm-lanbasek9-mz...
Loading mirage/switch/bin/c2960sm-lanbasek9-mz.image from 172.16.1.100 (via
FastEthernet0/24):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!
[OK - 4814025 bytes]

4814025 bytes copied in 99.481 secs (48391 bytes/sec)
Switch#
```

Troubleshooting the Cisco Enhanced EtherSwitch Service Module Software

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

Recovering from a Corrupted Software Image Using Xmodem

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

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

The Cisco enhanced EtherSwitch service module software can be corrupted while upgrading the software, by downloading the wrong file to the Cisco enhanced EtherSwitch service module, and by deleting the image file. In all of these cases, the service module does not pass the power-on self-test (POST) and there is no connectivity.

This procedure uses the Xmodem Protocol to recover from a corrupt or wrong image file. Many software packages support the Xmodem Protocol, and this procedure is largely dependent on the emulation software you are using.

To start the Xmodem protocol process, issue the **password reset** command. After you issue the **password reset** command, the following message appears:

```
Password reset process is complete...


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
    load_helper
    boot


Switch:
```

Restrictions

This procedure is recommended only for recovery of a corrupted image. To perform this procedure, the Cisco enhanced EtherSwitch service module must be at the boot loader prompt, and the console from the router to the Cisco enhanced EtherSwitch service module must be disconnected for the Xmodem Protocol to work.

SUMMARY STEPS

1. **service-module** *interface slot/port* **password-reset**
2. **flash_init**
3. **control+shift+6 x (**Use **x** to get back to the router prompt.)
4. **disconnect**
5. **copy flash: xmodem:** or **copy tftp: xmodem:**
6. **service-module** *interface slot/port* **session**
7. **dir flash:**
8. **boot flash:***image*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**service-module** *interface slot/port* **password-reset** **Example:** `Router# service-module gigabitethernet2/0 password-reset`	Ensures that the switch stays at the boot loader prompt, so that you can copy a new image through the Xmodem Protocol.
Step 2	**flash_init** **Example:** `Switch: flash_init`	Initializes the flash memory file system on the switch.
Step 3	**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. (Use **x** to get back to the router prompt.)
Step 4	**disconnect** **Example:** `Router#` **disconnect 1**	Disconnects the switch session to begin the Xmodem download.
Step 5	**copy flash: xmodem:** **Example:** `Router#` **copy flash: xmodem:** `or` **copy tftp: xmodem:** **Example:** `Router#` **copy tftp: xmodem:**	Starts the file transfer from the router flash memory by using the Xmodem Protocol from the router prompt. **Note** Use this command to download the software image from the router flash memory. Use this command from the router prompt. or Starts the file transfer from a TFTP server from the router prompt. **Note** Use this command to download the software image from a TFTP server. Use this command only if the image is not on the router flash memory.
Step 6	**service-module** *interface slot/port* **session** **Example:** `Router# service-module gigabitethernet1/0 session`	Connects to the service module and opens a Cisco enhanced EtherSwitch service module session.
Step 7	**dir flash:** **Example:** `switch: dir flash:`	Displays a list of all files and directories in flash memory on the service module.
Step 8	**boot flash:***image* **Example:** `switch> boot flash:c2960sm-lanbasek9-mz.image`	Boots the Cisco enhanced EtherSwitch service module image if all files and directories are in flash memory on the service module.

Troubleshooting

If the downloaded image (files and directories) are not in flash memory on the Cisco enhanced EtherSwitch service module, repeat Step 1 through Step 6. If the procedure fails again, ensure that your TFTP connection is up and that your TFTP session is open when you download the image.

Examples

This section provides the following examples:

Sample Output for the copy flash: xmodem Command

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

```
Router# copy flash: xmodem

**** WARNING ****
x/ymodem is a slow transfer protocol limited to the current speed
settings of the auxiliary/console ports. The use of the auxiliary
port for this download is strongly recommended.
During the course of the download no exec input/output will be
available.
---- ******* ----

Proceed? [confirm]
```

You are prompted for the source filename and destination filename:

```
Source filename [loader_bs.img]?
Destination filename [loader_bs.img]?
```

You are prompted for the Cisco enhanced EtherSwitch service module slot number:

```
Service Module slot number? [1]:
```

You are prompted for the service module interface number. Accept the default:

```
Service Module interface number? [0]:
```

You are prompted to confirm the buffer. Accept the default:

```
1k buffer? [confirm]
```

You are prompted for the max retry count. Accept the default:

```
Max Retry Count [10]:
```

You are prompted to confirm the transfer to the Cisco enhanced EtherSwitch service module:

```
Xmodem send on slot 2 interface 0. Please be sure there is enough space on receiving side.
Continue? [confirm]
```

The following appears when the image is downloaded to the service module:

```
Ready to send
file...........C!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!
262144 bytes copied in 101.744 secs (2577 bytes/sec)
```

Sample Output for the copy tftp: xmodem: Command

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

```
Router# copy tftp: xmodem:

**** WARNING ****
x/ymodem is a slow transfer protocol limited to the current speed
settings of the auxiliary/console ports. The use of the auxiliary
port for this download is strongly recommended.
During the course of the download no exec input/output will be
available.
---- ******* ----

Proceed? [confirm]
```

You are prompted for the IP address of the TFTP server:

```
Address or name of remote host []? 223.255.254.254
```

You are prompted for the source filename and destination filename:

```
Source filename [loader_bs.img]?
Destination filename [loader_bs.img]?
```

The following appears when you are connected to the TFTP server:

```
Accessing tftp://223.255.254.254/anyname/loader_bs.img...
```

You are prompted for the Cisco enhanced EtherSwitch service module slot number:

```
Service Module slot number? [1]:2
```

You are prompted for the service module interface number. Accept the default:

```
Service Module interface number? [0]:
```

You are prompted to confirm the buffer. Accept the default:

```
1k buffer? [confirm]
```

You are prompted for the max retry count. Accept the default:

```
Max Retry Count [10]:
```

You are prompted to confirm the transfer to the Cisco enhanced EtherSwitch service module:

```
Xmodem send on slot 2 interface 0. Please be sure there is enough space on receiving side.
Continue? [confirm]
```

The following appears when the image is downloaded to the service module:

```
Ready to send file...........
```

```
Loading anyname/loader_bs.img from 223.255.254.254 (via
GigabitEthernet0/0):!C!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!
!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!.!!!!!!.!!!!!!!!!!!!!!!!!!!!!
[OK - 262144 bytes]
!

Verifying checksum...  OK (0x4F76)
262144 bytes copied in 22.368 secs (11720 bytes/sec)
```

Sample Output for the service-module session Command on the Cisco Enhanced EtherSwitch Service Module

The following example shows what appears when you enter the **service-module session** command:

```
Router# service-module gigabitethernet1/0 session
Trying 41.0.0.1, 2130 ... Open

Switch:
```

Sample Output for the dir flash: Command on the Cisco Enhanced EtherSwitch Service Module

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

```
Switch: dir flash:
Directory of flash:/

4  -rwx        2056   Mar 1 2008 00:01:29 +00:00  vlan.dat
6  -rwx     6636204   Mar 1 2008 00:19:19 +00:00 c3560e-universalk9-mz
   7  -rwx        1709  Jan 12 2009 00:56:39 +00:00  config.text
   8  -rwx           5  Jan 12 2009 00:56:39 +00:00  private-config.text

32514048 bytes total (19113472 bytes free)
```

Sample Output for the service-module password-reset Command on the Cisco Enhanced EtherSwitch Service Module

The following example shows what appears when you enter the **service-module password-reset** command:

```
Router# service-module gigabitethernet2/0 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
Router#
[Resuming connection 1 to 100.0.2.1 ... ]

Password reset process is complete...

Base ethernet MAC Address: 00:00:00:20:60:80
Xmodem file system is available.
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
   load_helper
   boot

Router:
```

Sample Output for the flash_init Command on the Cisco Enhanced EtherSwitch Service Module

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

```
Switch: flash_init
Initializing Flash...
flashfs[0]:7 files, 1 directories
flashfs[0]:Total bytes:32514048
flashfs[0]:Bytes used:13400576
flashfs[0]:Bytes available:19113472
flashfs[0]:flashfs fsck took 18 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs) installed, fsid:3
Setting console baud rate to 9600...
```

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 enhanced EtherSwitch service module 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 enhanced EtherSwitch service modules 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 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 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 10	**reload** **Example:** `Switch# reload`	Reloads the switch.

Example

Sample Output for Recovering from a Lost or Forgotten Password

```
Router#service-module g2/0 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
Router#service g2/0 session
Trying 20.1.1.1, 2131 ... Open

Using driver version 1 for media type 1
Base ethernet MAC Address: 00:24:c4:71:e3:00
Xmodem file system is available.
The password-recovery mechanism is enabled.


Password reset process is complete...


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: flash_init
Initializing Flash...
mifs[2]: 0 files, 1 directories
mifs[2]: Total bytes     :    3870720
mifs[2]: Bytes used      :       1024
```

```
mifs[2]: Bytes available :    3869696
mifs[2]: mifs fsck took 0 seconds.
mifs[3]: 5 files, 1 directories
mifs[3]: Total bytes     :   61028352
mifs[3]: Bytes used      :    8372224
mifs[3]: Bytes available :   52656128
mifs[3]: mifs fsck took 4 seconds.
...done Initializing Flash.

switch:
switch: dir flash:
Directory of flash:/

    2  -rwx  8293503   <date>               c2960sm-lanbasek9-mz.DT05292009
    3  -rwx  676       <date>               vlan.dat
    4  -rwx  2072      <date>               multiple-fs
    5  -rwx  2118      <date>               config.text
    6  -rwx  1921      <date>               private-config.text

52656128 bytes available (8372224 bytes used)

switch: rename flash:config.text flash:config.text.old

switch: boot
Loading
"flash:/c2960sm-lanbasek9-mz.DT05292009"...@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "flash:/c2960sm-lanbasek9-mz.DT05292009" 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



Cisco IOS Software, C2960SM Software (C2960SM-LANBASEK9-M), Experimental Version
12.2(20090420:202439) [giyoon-flo_ee_l 221]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 29-May-09 15:43 by giyoon
Image text-base: 0x00003000, data-base: 0x01500000

Initializing flashfs...
Using driver version 1 for media type 1
mifs[3]: 0 files, 1 directories
mifs[3]: Total bytes     : 3870720
mifs[3]: Bytes used      : 1024
mifs[3]: Bytes available : 3869696
mifs[3]: mifs fsck took 0 seconds.
mifs[3]: Initialization complete.

mifs[4]: 5 files, 1 directories
```

```
mifs[4]: Total bytes     : 61028352
mifs[4]: Bytes used      : 8372224
mifs[4]: Bytes available : 52656128
mifs[4]: mifs fsck took 0 seconds.
mifs[4]: Initialization complete.

...done Initializing flashfs.

POST: CPU MIC register Tests : Begin
POST: CPU MIC register Tests : End, Status Passed

POST: MA BIST : Begin
POST: MA BIST : End, Status Passed

POST: TCAM BIST : Begin
POST: TCAM BIST : End, Status Passed

POST: CPU MIC interface Loopback Tests : Begin
POST: CPU MIC interface Loopback Tests : End, Status Passed

POST: PortASIC RingLoopback Tests : Begin
POST: PortASIC RingLoopback Tests : End, Status Passed

front_end/ (directory)
extracting front_end/fe_type_4 (76512 bytes)
extracting front_end/front_end_ucode_info (129 bytes)
extracting front_end/fe_type_3 (76512 bytes)
extracting front_end/fe_type_2 (76512 bytes)
extracting ucode_info (76 bytes)
POST: PortASIC Port Loopback Tests : Begin
POST: PortASIC Port Loopback Tests : End, Status Passed

Waiting for Port download...Complete


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.

cisco SM-ES2-24 (PowerPC405) processor with 131072K bytes of memory.
Processor board ID FHH130400FM
Last reset from power-on
Target IOS Version 12.2(52)EX
1 Virtual Ethernet interface
23 FastEthernet interfaces
3 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:24:C4:71:E3:00
Motherboard serial number       : FHH130400FM
Model number                    : SM-ES2-24
System serial number            : FHH130400FM
```

```
Hardware Board Revision Number  : 0x00


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    SM-ES2-24          12.2(20090420:202439) C2960SM-LANBASEK9-M



Press RETURN to get started!


*Mar  1 00:00:39.241: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to down
*Mar  1 00:00:39.443: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Mar  1 00:00:58.921: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960SM Software (C2960SM-LANBASEK9-M), Experimental Version
12.2(20090420:202439) [giyoon-flo_ee_l 221]
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Fri 29-May-09 15:43 by giyoon
*Mar  1 00:01:00.834: %LINK-3-UPDOWN: Interface GigabitEthernet0/26, changed state to up
*Mar  1 00:01:00.842: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/26,
changed state to up
*Mar  1 00:01:28.944: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up
*Apr 20 18:35:44.000: NRGYZ:ERROR:Could not notify EnergyWise of time setting change.
```

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. (Optional) **load_helper** *filesystem:/file-url ...*
5. **boot**
6. **enable**
7. **configure terminal**
8. **enable secret** *password*
9. **exit**
10. **copy running-configuration startup-configuration**
11. **reload**
12. (Optional) **set**

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 gigabitethernet1/0 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:** `rommon> dir flash:`	Displays a list of all files and directories in flash memory on the service module.
Step 4	**load_helper** ***filesystem:/file-url ...*** **Example:** `Switch: load_helper flash: xyz`	Loads and initializes one or more helper images.
Step 5	**boot** **Example:** `Switch: boot`	Boots the system.
Step 6	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode from the service module prompt.
Step 7	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 8	**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.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Switch(config)# exit`	Returns you to privileged EXEC mode.
Step 10	**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 11	**reload** **Example:** `Switch# reload`	Reloads the switch. **Note** This does not set the environment variables if the switch is set to auto boot.
Step 12	**set** **Example:** `Switch# set`	Lists all environment variables, including the current baud rate.

Example

Sample Output for the set Command

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

```
Switch: set

BAUD=9600
MAC_ADDR=00:00:00:20:30:80
MANUAL_BOOT=yes
SDM_TEMPLATE_ID=0
SWITCH_NUMBER=2
SWITCH_PRIORITY=1
```

Cisco Enhanced EtherSwitch Service Module Features

The following features are available on the Cisco enhanced EtherSwitch service modules.

Features for Layer 2 Enhanced EtherSwitch Service Modules

Note The features listed in this section are specific to the following enhanced EtherSwitch service modules: SM-ES2-16-P, SM-ES2-24, SM-ES2-24-P, and SM-D-ES2-48.

Some features described in this section are available only on the cryptographic (supports encryption) version of the software. You must obtain authorization to use this feature and to download the cryptographic version of the software from Cisco.com. For more information, see the release notes for this release.

The enhanced EtherSwitch service module has these features:

Ease-of-Deployment and Ease-of-Use Features

The enhanced EtherSwitch service module ships with these features to make the deployment and the use easier:

- Express Setup for quickly configuring an enhanced EtherSwitch service module for the first time with basic IP information, contact information, Express Setup for quickly configuring an enhanced EtherSwitch service module for the first time with basic IP information, contact information, Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see the getting started guide.
- User-defined and Cisco-default Smartports macros for creating custom enhanced EtherSwitch service module configurations for simplified deployment across the network.
- An embedded device manager GUI for configuring and monitoring a single enhanced EtherSwitch service module through a web browser. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the enhanced EtherSwitch service module online help.

- Cisco Network Assistant (hereafter referred to as *Network Assistant*) for
  - Accomplishing multiple configuration tasks from a single graphical interface without needing to remember command-line interface (CLI) commands to accomplish specific tasks.
  - Interactive guide mode that guides you in configuring complex features such as VLANs, ACLs, and quality of service (QoS).
  - Configuration wizards that prompt you to provide only the minimum required information to configure complex features such as QoS priorities for traffic, priority levels for data applications, and security.
  - Downloading an image to an enhanced EtherSwitch service module.
  - Applying actions to multiple ports and multiple switches at the same time, such as VLAN and QoS settings, inventory and statistic reports, link- and enhanced EtherSwitch service module-level monitoring and troubleshooting, and multiple switch software upgrades.
  - Monitoring real-time status of an enhanced EtherSwitch service module or multiple switches from the LEDs on the front-panel images. The system, redundant power system (RPS), and port LED colors on the images are similar to those used on the physical LEDs.

Note To use RPS, the enhanced EtherSwitch service module must be running the LAN Base image.

Performance Features

The enhanced EtherSwitch service module ships with these performance features:

- Autosensing of port speed and autonegotiation of duplex mode on all enhanced EtherSwitch service module ports for optimizing bandwidth
- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 Mb/s that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately
- Support for up to 9000 bytes for frames that are bridged in hardware, and up to 2000 bytes for frames that are bridged by software
- IEEE 802.3x flow control on all ports (the enhanced EtherSwitch service module does not send pause frames)
- EtherChannel for enhanced fault tolerance and for providing up to 8 Gb/s (Gigabit EtherChannel) or 800 Mb/s (Fast EtherChannel) full-duplex bandwidth among switches, routers, and servers
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links
- Forwarding of Layer 2 packets at Gigabit line rate
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3 for efficiently forwarding multimedia and multicast traffic
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)

- IGMP snooping querier support to configure enhanced EtherSwitch service module to generate periodic IGMP general query messages
- IPv6 host support for basic IPv6 management
- Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP version 6 (IPv6) multicast data to clients and routers in a switched network

Note To use IPv6 features, the enhanced EtherSwitch service module must be running the LAN Base image.

- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons

Note To use MVR, the enhanced EtherSwitch service module must be running the LAN Base image.

- IGMP filtering for controlling the set of multicast groups to which hosts on an enhanced EtherSwitch service module port can belong
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP leave timer for configuring the leave latency for the network
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features
- Support for Cisco IOS IP Service Level Agreements (SLAs) responder that allows the system to anticipate and respond to Cisco IOS IP SLAs request packets for monitoring network performance. See the release notes for responder configuration
- Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold)
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure

Note To use Flex Link Multicast Fast Convergence, the enhanced EtherSwitch service module must be running the LAN Base image.

Management Options

These are the options for configuring and managing the enhanced EtherSwitch service module:

- An embedded device manager—The device manager is a GUI that is integrated in the software image. You use it to configure and to monitor a single enhanced EtherSwitch service module. For information about launching the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
- Network Assistant—Network Assistant is a network management application that can be downloaded from Cisco.com. You use it to manage a single enhanced EtherSwitch service module, a cluster of switches, or a community of devices. For more information about Network Assistant, see *Getting Started with Cisco Network Assistant*, available on Cisco.com.

- CLI—The Cisco IOS software supports desktop- and multilayer-switching features. You can access the CLI either by connecting your management station directly to the enhanced EtherSwitch service module console port or by using Telnet from a remote management station. For more information about the CLI, see the Using the Command-Line Interface chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- SNMP—SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The enhanced EtherSwitch service module supports a comprehensive set of MIB extensions and four remote monitoring (RMON) groups. For more information about using SNMP, see the Configuring SNMP chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- CNS—Cisco Networking Services is network management software that acts as a configuration service for automating the deployment and management of network devices and services. You can automate initial configurations and configuration updates by generating enhanced EtherSwitch service module-specific configuration changes, sending them to the enhanced EtherSwitch service module, executing the configuration change, and logging the results.

  For more information about CNS, see the Configuring Cisco IOS CNS Agents chapter in *Catalyst 2960 Switch Software Configuration Guide*.

Manageability Features

These are the manageability features:

- CNS embedded agents for automating enhanced EtherSwitch service module management, configuration storage, and delivery
- DHCP for automating configuration of enhanced EtherSwitch service module information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
- DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches
- DHCP server port-based address allocation for the preassignment of an IP address to an enhanced EtherSwitch service module port
- Directed unicast requests to a DNS server for identifying an enhanced EtherSwitch service module through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying an enhanced EtherSwitch service module through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table
- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the enhanced EtherSwitch service module and other Cisco devices on the network
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones

Note To use LLDP-MED, the enhanced EtherSwitch service module must be running the LAN Base image.

- LLDP media extensions (LLDP-MED) location TLV that provides location information from the enhanced EtherSwitch service module to the endpoint device
- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the enhanced EtherSwitch service module uses
- Support for the SSM PIM protocol to optimize multicast applications, such as video
- Source Specific Multicast (SSM) mapping for multicast applications provides a mapping of source to group, allowing listeners to connect to multicast sources dynamically and reduces dependencies on the application
- Support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 to utilize IPv6 transport, communicate with IPv6 peers, and advertise IPv6 routes
- Support for these IP services, making them VRF aware so that they can operate on multiple routing instances: HSRP, GLBP, uRPF, ARP, SNMP, IP SLA, TFTP, FTP, syslog, traceroute, and ping
- Configuration logging to log and to view changes to the enhanced EtherSwitch service module configuration
- Unique device identifier to provide product identification information through a **show inventory** user EXEC command display
- In-band management access through the device manager over a Netscape Navigator or Microsoft Internet Explorer browser session
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic versions of the software)
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the enhanced EtherSwitch service module console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying enhanced EtherSwitch service module configuration or enhanced EtherSwitch service module image files (requires the cryptographic version of the software)
- Configuration replacement and rollback to replace the running configuration on an enhanced EtherSwitch service module with any saved Cisco IOS configuration file
- The HTTP client in Cisco IOS supports can send requests to both IPv4 and IPv6 HTTP server, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients
- Simple Network and Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can send SNMP queries and receive SNMP notifications from a device running IPv6
- IPv6 stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses
- Disabling MAC address learning on a VLAN

- DHCP server port-based address allocation for the preassignment of an IP address to an enhanced EtherSwitch service module port.

Availability and Redundancy Features

These are the availability and redundancy features:

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  - Up to 128 spanning-tree instances supported
  - Per-VLAN spanning-tree plus (PVST+) for load balancing across VLANs
  - Rapid PVST+ for load balancing across VLANs and providing rapid convergence of spanning-tree instances
  - UplinkFast and BackboneFast for fast convergence after a spanning-tree topology change and for achieving load balancing between redundant uplinks, including Gigabit uplinks
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state
  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs
  - Root guard for preventing switches outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link
- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy

Note To use Flex Links, the enhanced EtherSwitch service module must be running the LAN Base image.

- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another Cisco enhanced EtherSwitch service module.

Note To use Link-state Tracking, the enhanced EtherSwitch service module must be running the LAN Base image.

VLAN Features

These are the VLAN features:

- Support for up to 255 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the 1 to 4094 range as allowed by the IEEE 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (IEEE 802.1Q) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
- Voice VLAN for creating subnets for voice traffic from Cisco IP Phones
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The enhanced EtherSwitch service module CPU continues to send and receive control protocol frames.
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

Note To use VLAN Flex Link Load Balancing, the enhanced EtherSwitch service module must be running the LAN Base image.

Security Features

The enhanced EtherSwitch service module ships with these security features:

- IP Service Level Agreements (IP SLAs) responder support that allows the enhanced EtherSwitch service module to be a target device for IP SLAs active traffic monitoring

  Note To use IP SLAs, the enhanced EtherSwitch service module must be running the LAN Base image.

- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser

  Note To use Web Authentication, the enhanced EtherSwitch service module must be running the LAN Base image.

- Local web authentication banner so that a custom banner or an image file can be displayed at a web authentication login screen
- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute

Note To use this feature, the enhanced EtherSwitch service module must be running the LAN Base image.

- Password-protected access (read-only and read-write access) to management interfaces (device manager, Network Assistant, and the CLI) for protection against unauthorized configuration changes
- Multilevel security for a choice of security level, notification, and resulting actions
- Static MAC addressing for ensuring security
- Protected port option for restricting the forwarding of traffic to designated ports on the same enhanced EtherSwitch service module
- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port
- VLAN aware port security option to shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port.
- Port security aging to set the aging time for secure addresses on a port
- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs
- Standard and extended IP access control lists (ACLs) for defining inbound security policies on Layer 2 interfaces (port ACLs)
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- Source and destination MAC-based ACLs for filtering non-IP traffic
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers
- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:

  Note To use MDA, the enhanced EtherSwitch service module must be running the LAN Base image.

  – VLAN assignment for restricting IEEE 802.1x-authenticated users to a specified VLAN
  – Port security for controlling access to IEEE 802.1x ports
  – Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port
  – IP phone detection enhancement to detect and recognize a Cisco IP phone.
  – Guest VLAN to provide limited services to non-IEEE 802.1x-compliant users
  – Restricted VLAN to provide limited services to users who are IEEE 802.1x compliant, but do not have the credentials to authenticate via the standard IEEE 802.1x processes

  Note To use authentication with restricted VLANs, the enhanced EtherSwitch service module must be running the LAN Base image.

  – IEEE 802.1x accounting to track network usage

  - IEEE 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame

Note To use authentication with wake-on-LAN, the enhanced EtherSwitch service module must be running the LAN Base image.

- IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the enhanced EtherSwitch service module

Note To use IEEE 802.1x readiness check, the enhanced EtherSwitch service module must be running the LAN Base image.

- Voice aware IEEE 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs.

Note To use voice aware IEEE 802.1x authentication, the enhanced EtherSwitch service module must be running the LAN Base image.

- MAC authentication bypass to authorize clients based on the client MAC address.

Note To use MAC authentication bypass, the enhanced EtherSwitch service module must be running the LAN Base image.

- Network Admission Control (NAC) Layer 2 IEEE 802.1x validation of the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access.

  For information about configuring NAC Layer 2 IEEE 802.1x validation, see the Configuring NAC Layer 2 IEEE 802.1x Validation section in *Catalyst 2960 Switch Software Configuration Guide*.

Note To use NAC, the enhanced EtherSwitch service module must be running the LAN Base image.

- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services
- Secure Socket Layer (SSL) Version 3.0 support for the HTTP 1.1 server authentication, encryption, and message integrity and HTTP client authentication to allow secure HTTP communications (requires the cryptographic version of the software)
- IEEE 802.1x Authentication with ACLs and the RADIUS Filter-Id Attribute

QoS and CoS Features

These are the QoS and CoS features:

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues

  Note To use auto-QoS, the enhanced EtherSwitch service module must be running the LAN Base image.

- Classification
  - IP type-of-service/Differentiated Services Code Point (IP ToS/DSCP) and IEEE 802.1p CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications

    Note To use DSCP, the enhanced EtherSwitch service module must be running the LAN Base image.

  - IP ToS/DSCP and IEEE 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network

    Note To use flow-based packet classification, the enhanced EtherSwitch service module must be running the LAN Base image.

  - Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain
  - Trusted boundary for detecting the presence of a Cisco IP Phone, trusting the CoS value received, and ensuring port security
- Policing

  Note To use policy maps, the enhanced EtherSwitch service module must be running the LAN Base image

  - Traffic-policing policies on the enhanced EtherSwitch service module port for managing how much of the port bandwidth should be allocated to a specific traffic flow
  - In Cisco IOS Release 12.2(25)SED and later, iIf you configure multiple class maps for a hierarchical policy map, each class map can be associated with its own port-level (second-level) policy map. Each second-level policy map can have a different policer.
  - Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates
- Out-of-Profile
  - Out-of-profile markdown for packets that exceed bandwidth utilization limits
- Ingress queueing and scheduling

  - Two configurable ingress queues for user traffic (one queue can be the priority queue)
  - Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications

Note To use WTD, the enhanced EtherSwitch service module must be running the LAN Base image.

  - Shaped round robin (SRR) as the scheduling service for specifying the rate at which packets are sent to the internal ring (sharing is the only supported mode on ingress queues)

Note To use ingress queueing, the enhanced EtherSwitch service module must be running the LAN Base image.

- Egress queues and scheduling
  - Four egress queues per port
  - WTD as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - SRR as the scheduling service for specifying the rate at which packets are dequeued to the egress interface (shaping or sharing is supported on egress queues). Shaped egress queues are guaranteed but limited to using a share of port bandwidth. Shared egress queues are also guaranteed a configured share of bandwidth, but can use more than the guarantee if other queues become empty and do not use their share of the bandwidth.

Note To use egress queueing, the enhanced EtherSwitch service module must be running the LAN Base image.

Monitoring Features

These are the monitoring features:

- enhanced EtherSwitch service module LEDs that provide status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the enhanced EtherSwitch service module has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN
- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device
- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on 10/100 and 10/100/1000 copper Ethernet ports

Default Settings After Initial Layer 2 Enhanced EtherSwitch Service Module Configuration

The enhanced EtherSwitch service module is designed for plug-and-play operation, requiring only that you assign basic IP information to the enhanced EtherSwitch service module and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

Note For information about assigning an IP address by using the browser-based Express Setup program, see the getting started guide. For information about assigning an IP address by using the CLI-based setup program, see the hardware installation guide.

If you do not configure the enhanced EtherSwitch service module at all, the enhanced EtherSwitch service module operates with these default settings:

- Default enhanced EtherSwitch service module IP address, subnet mask, and default gateway is 0.0.0.0. For more information, see the Assigning the Switch IP Address and Default Gateway chapter and the Configuring DHCP Features chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- Default domain name is not configured. For more information, see the Assigning the Switch IP Address and Default Gateway chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- DHCP client is enabled, the DHCP server is enabled (only if the device acting as a DHCP server is configured and is enabled), and the DHCP relay agent is enabled (only if the device is acting as a DHCP relay agent is configured and is enabled). For more information, see the Assigning the Switch IP Address and Default Gateway chapter and the Configuring DHCP Features chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- No passwords are defined. For more information, see the Administering the Switch chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- System name and prompt is *Switch*. For more information, see the Administering the Switch chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- NTP is enabled. For more information, see the Administering the Switch chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- DNS is enabled. For more information, see the Administering the Switch chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- TACACS+ is disabled. For more information, see the Configuring Switch-Based Authentication chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- RADIUS is disabled. For more information, see the Configuring Switch-Based Authentication chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see the Configuring Switch-Based Authentication chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- IEEE 802.1x is disabled. For more information, see the Configuring IEEE 802.1x Port-Based Authentication chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- Port parameters
  - Interface speed and duplex mode is autonegotiate. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 2960 Switch Software Configuration Guide*.

  - Auto-MDIX is enabled. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - Flow control is off. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - PoE is autonegotiate. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- VLANs
  - Default VLAN is VLAN 1. For more information, see the Configuring VLANs chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - VLAN trunking setting is dynamic auto (DTP). For more information, see the Configuring VLANs chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - Trunk encapsulation is negotiate. For more information, see the Configuring VLANs chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - VTP mode is server. For more information, see the Configuring VTP chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - VTP version is Version 1. For more information, see the Configuring VTP chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - Voice VLAN is disabled. For more information, see the Configuring Voice VLAN chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- STP, PVST+ is enabled on VLAN 1. For more information, see the Configuring STP chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- MSTP is disabled. For more information, see the Configuring MSTP chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- Optional spanning-tree features are disabled. For more information, see the Configuring Optional Spanning-Tree Features chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- Flex Links are not configured. For more information, see the Configuring Flex Links and the MAC Address-Table Move Update Feature chapter in *Catalyst 2960 Switch Software Configuration Guide*.

Note To use Flex Links, the switch must be running the LAN Base image.

- DHCP snooping is disabled. The DHCP snooping information option is enabled. For more information, see the Configuring DHCP Features chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- IGMP throttling setting is deny. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- The IGMP snooping querier feature is disabled. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- MVR is disabled. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 2960 Switch Software Configuration Guide*.

Note To use MVR, the switch must be running the LAN Base image.

- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - No protected ports are defined. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - Unicast and multicast traffic flooding is not blocked. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 2960 Switch Software Configuration Guide*.
  - No secure ports are configured. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- CDP is enabled. For more information, see the Configuring CDP chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- UDLD is disabled. For more information, see the Configuring UDLD chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- SPAN and RSPAN are disabled. For more information, see the Configuring SPAN and RSPAN chapter in *Catalyst 2960 Switch Software Configuration Guide*.

Note To use RSPAN, the switch must be running the LAN Base image.

- RMON is disabled. For more information, see the Configuring RMON chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- Syslog messages are enabled and appear on the console. For more information, see the Configuring System Message Logging chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- SNMP is enabled (Version 1). For more information, see the Configuring SNMP chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- No ACLs are configured. For more information, see the Configuring Network Security with ACLs chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- QoS is disabled. For more information, see the Configuring QoS chapter in *Catalyst 2960 Switch Software Configuration Guide*.
- No EtherChannels are configured. For more information, see the Configuring EtherChannels and Link-State Tracking chapter in *Catalyst 2960 Switch Software Configuration Guide*.

Features for Layer 2 and Layer 3 Enhanced EtherSwitch Service Modules

Note The features listed in this section are specific to the following enhanced EtherSwitch service modules: SM-ES3-16-P, SM-ES3G-16-P, SM-ES3-24-P, SM-ES3G-24-P, and SM-D-ES3-48-P, and SM-D-ES3G-48-P.

The enhanced EtherSwitch service module has these features:

- Deployment Features, page 50
- Performance Features, page 50
- Management Options, page 52
- Manageability Features, page 52 (includes a feature requiring the cryptographic universal software image)
- Availability and Redundancy Features, page 54
- VLAN Features, page 55
- Security Features, page 55 (includes a feature requiring the cryptographic universal software image)
- QoS and CoS Features, page 57
- Layer 3 Features, page 58 (includes features requiring the IP services feature set)
- Power over Ethernet Features, page 59
- Monitoring Features, page 60

The enhanced EtherSwitch service module supports either the cryptographic (supports encryption) or the noncryptographic universal software image. The universal software image supports the IP base and IP services. You must have a Cisco IOS software license for a specific feature set to enable it. For more information about the software license, see the *Cisco Software Activation and Compatibility Document* document on Cisco.com.

Some features described in this chapter are only available on the cryptographic software image. You must obtain authorization to use these features and to download the cryptographic software from Cisco.com. For more information, see the release notes for this release.

The enhanced EtherSwitch service module supports one of these feature sets:

- IP base feature set, which provides Layer 2+ features (enterprise-class intelligent services). These features include access control lists (ACLs), quality of service (QoS), static routing, EIGRP stub routing, PIM stub routing, the Hot Standby Router Protocol (HSRP), Routing Information Protocol (RIP), and basic IPv6 management. Switches with the IP base feature set can be upgraded to the IP services feature set.
- IP services feature set, which provides a richer set of enterprise-class intelligent services. It includes all IP base features plus full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging). The IP services feature set includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and the Open Shortest Path First (OSPF) Protocol. This feature set also supports IPv6 access control lists (ACLs) and Multicast Listener Discovery (MLD) snooping.

Note Unless otherwise noted, all features described in this section are supported on both the IP base and IP services feature sets.

Deployment Features

The enhanced EtherSwitch service module ships with these features:

- Express Setup for quickly configuring an enhanced EtherSwitch service module for the first time with basic IP information, contact information, enhanced EtherSwitch service module and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see *Catalyst 3560-E Switch Getting Started Guide*.
- User-defined and Cisco-default Smartports macros for creating custom enhanced EtherSwitch service module configurations for simplified deployment across the network.
- An embedded device manager GUI for configuring and monitoring a single enhanced EtherSwitch service module through a web browser. For information about starting the device manager, see *Catalyst 3560-E Switch Getting Started Guide*. For more information about the device manager, see the enhanced EtherSwitch service module online help.
- Cisco Network Assistant (referred to as *Network Assistant*) for
  - Accomplishing multiple configuration tasks from a single graphical interface without needing to remember CLI commands to accomplish specific tasks.
  - Interactive guide mode that guides you in configuring complex features such as VLANs, ACLs, and quality of service (QoS).
  - Configuration wizards that prompt you to provide only the minimum required information to configure complex features such as QoS priorities for video traffic, priority levels for data applications, and security.
  - Downloading an image to an enhanced EtherSwitch service module.
  - Applying actions to multiple ports and multiple switches at the same time, such as VLAN and QoS settings, inventory and statistic reports, link- and enhanced EtherSwitch service module-level monitoring and troubleshooting, and multiple enhanced EtherSwitch service module software upgrades.
  - Monitoring real-time status of an enhanced EtherSwitch service module or multiple switches from the LEDs on the front-panel images. The system, redundant power system (RPS), system and port LED colors on the images are similar to those used on the physical LEDs.

Note For network configuration examples showing design concepts, establishing a small- to medium-sized, and large networks using Layer 2 and Layer 3 enhanced EtherSwitch service modules, see *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.

Performance Features

The enhanced EtherSwitch service module ships with these performance features:

- Autosensing of port speed and autonegotiation of duplex mode on all enhanced EtherSwitch service module ports for optimizing bandwidth
- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 10/100- and 10/100/1000-Mb/s interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately
- Support for the maximum packet size or maximum transmission unit (MTU) size for these types of frames:

  - Up to 9216 bytes for routed frames
  - Up to 9216 bytes for frames that are bridged in hardware and software through Gigabit Ethernet ports
- IEEE 802.3x flow control on all ports (the enhanced EtherSwitch service module does not send pause frames)
- Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links
- Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Cisco Group Management Protocol (CGMP) server support and Internet Group Management Protocol (IGMP) snooping for IGMP Versions 1, 2, and 3:
  - (For CGMP devices) CGMP for limiting multicast traffic to specified end stations and reducing overall network traffic
  - (For IGMP devices) IGMP snooping for efficiently forwarding multimedia and multicast traffic
- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure enhanced EtherSwitch service module to generate periodic IGMP General Query messages
- IIGMP Helper to allow the enhanced EtherSwitch service module to forward a host request to join a multicast stream to a specific IP destination address
- Multicast Listener Discovery (MLD) snooping to enable efficient distribution of IP Version 6 (IPv6) multicast data to clients and routers in a switched network.
- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons
- IGMP filtering for controlling the set of multicast groups to which hosts on an enhanced EtherSwitch service module port can belong
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP leave timer for configuring the leave latency for the network
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features
- Web Cache Communication Protocol (WCCP) for redirecting traffic to wide-area application engines, for enabling content requests to be fulfilled locally, and for localizing web-traffic patterns in the network (requires the IP services feature set)
- Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold)
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure
- Support for IEEE 802.11n-enabled access points and support for powered devices that draw more than 15.4 watts

Management Options

These are the options for configuring and managing the enhanced EtherSwitch service module:

- An embedded device manager—The device manager is a GUI that is integrated in the universal software image. You use it to configure and to monitor a single enhanced EtherSwitch service module. For information about starting the device manager, see the getting started guide. For more information about the device manager, see the switch online help.
- Network Assistant—Network Assistant is a network management application that can be downloaded from Cisco.com. You use it to manage a single switch, a cluster of switches, or a community of devices. For more information about Network Assistant, see *Getting Started with Cisco Network Assistant*, available on Cisco.com.
- SNMP—SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station or a PC that is running platforms such as HP OpenView or SunNet Manager. The enhanced EtherSwitch service module supports a comprehensive set of MIB extensions and four remote monitoring (RMON) groups.
- CNS—Cisco Networking Services is network management software that acts as a configuration service for automating the deployment and management of network devices and services. You can automate initial configurations and configuration updates by generating enhanced EtherSwitch service module-specific configuration changes, sending them to the enhanced EtherSwitch service module, executing the configuration change, and logging the results.

  For more information about CNS, see *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.

Manageability Features

These are the manageability features:

- CNS embedded agents for automating enhanced EtherSwitch service module management, configuration storage, and delivery
- DHCP for automating configuration of enhanced EtherSwitch service module information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
- DHCP server port-based address allocation for the preassignment of an IP address to an enhanced EtherSwitch service module port
- Directed unicast requests to a DNS server for identifying an enhanced EtherSwitch service module through its IP address and its corresponding hostname and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying an enhanced EtherSwitch service module through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table
- Disabling MAC address learning on a VLAN

- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the enhanced EtherSwitch service module and other Cisco devices on the network
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones
- Support for the LLDP-MED location TLV that provides location information from the enhanced EtherSwitch service module to the endpoint device
- Network Time Protocol (NTP) for providing a consistent time stamp to all switches from an external source
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the enhanced EtherSwitch service module uses
- Configuration logging to log and to view changes to the enhanced EtherSwitch service module configuration
- Configuration replacement and rollback to replace the running configuration on an enhanced EtherSwitch service module with any saved Cisco IOS configuration file
- Unique device identifier to provide product identification information through a **show inventory** user EXEC command display
- In-band management access through the device manager over a Netscape Navigator or Microsoft Internet Explorer browser session
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic universal software image)
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the enhanced EtherSwitch service module console port to a directly attached terminal or to a remote terminal through a serial connection or a modem
- Out-of-band management access through the Ethernet management port to a PC
- Secure Copy Protocol (SCP) feature to provide a secure and authenticated method for copying enhanced EtherSwitch service module configuration or enhanced EtherSwitch service module image files (requires the cryptographic universal software image)
- DHCP-based autoconfiguration and image update to download a specified configuration a new image to a large number of switches
- Source Specific Multicast (SSM) mapping for multicast applications to provide a mapping of source to allowing IGMPv2 clients to utilize SSM, allowing listeners to connect to multicast sources dynamically and reducing dependencies on the application
- The HTTP client in Cisco IOS supports can send requests to both IPv4 and IPv6 HTTP servers, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients
- Simple Network and Management Protocol (SNMP) can be configured over IPv6 transport so that an IPv6 host can send SNMP queries and receive SNMP notifications from a device running IPv6.
- IPv6 supports stateless autoconfiguration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses.
- Local web authentication banner so that custom banner or image file can be displayed at a web authentication login screen

Note For additional descriptions of the management interfaces, see *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.

Availability and Redundancy Features

These are the availability and redundancy features:

- HSRP for command enhanced EtherSwitch service module and Layer 3 router redundancy
- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- IEEE 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks. STP has these features:
  - Up to 128 spanning-tree instances supported
  - Per-VLAN spanning-tree plus (PVST+) for load-balancing across VLANs
  - Rapid PVST+ for load-balancing across VLANs and providing rapid convergence of spanning-tree instances
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) for grouping VLANs into a spanning-tree instance and for providing multiple forwarding paths for data traffic and load-balancing and rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree by immediately changing root and designated ports to the forwarding state
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP mode:
  - Port Fast for eliminating the forwarding delay by enabling a port to immediately change from the blocking state to the forwarding state
  - BPDU guard for shutting down Port Fast-enabled ports that receive bridge protocol data units (BPDUs)
  - BPDU filtering for preventing a Port Fast-enabled port from sending or receiving BPDUs
  - Root guard for preventing switches outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link
- Equal-cost routing for link-level and enhanced EtherSwitch service module-level redundancy
- Flex Link Layer 2 interfaces to back up one another as an alternative to STP for basic link redundancy
- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers and to allow the failover of the server traffic to an operational link on another Cisco enhanced EtherSwitch service module

VLAN Features

These are the VLAN features:

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the 1 to 4094 range as allowed by the IEEE 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- Inter-Switch Link (ISL) and IEEE 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- Dynamic Trunking Protocol (DTP) for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (IEEE 802.1Q or ISL) to be used
- VLAN Trunking Protocol (VTP) and VTP pruning for reducing network traffic by restricting flooded traffic to links destined for stations receiving the traffic
- Voice VLAN for creating subnets for voice traffic from Cisco IP Phones
- Dynamic voice virtual LAN (VLAN) for multidomain authentication (MDA) to allow a dynamic voice VLAN on an MDA-enabled port
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch CPU continues to send and receive control protocol frames.
- Private VLANs to address VLAN scalability problems, to provide a more controlled IP address allocation, and to allow Layer 2 ports to be isolated from other ports on the enhanced EtherSwitch service module
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

Security Features

The enhanced EtherSwitch service module ships with these security features:

- Web authentication to allow a supplicant (client) that does not support IEEE 802.1x functionality to be authenticated using a web browser.
- Password-protected access (read-only and read-write access) to management interfaces (device manager, Network Assistant, and the CLI) for protection against unauthorized configuration changes
- Multilevel security for a choice of security level, notification, and resulting actions
- Static MAC addressing for ensuring security
- Protected port option for restricting the forwarding of traffic to designated ports on the same enhanced EtherSwitch service module
- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port

- VLAN aware port security option to shut down the VLAN on the port when a violation occurs, instead of shutting down the entire port
- Port security aging to set the aging time for secure addresses on a port
- BPDU guard for shutting down a Port Fast-configured port when an invalid configuration occurs
- Standard and extended IP access control lists (ACLs) for defining security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers
- Source and destination MAC-based ACLs for filtering non-IP traffic
- IPv6 ACLs to be applied to interfaces to filter IPv6 traffic
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection to prevent malicious attacks on the enhanced EtherSwitch service module by not relaying invalid ARP requests and responses to other ports in the same VLAN
- IEEE 802.1Q tunneling so that customers with users at remote sites across a service-provider network can keep VLANs segregated from other customers and Layer 2 protocol tunneling to ensure that the customer's network has complete STP, CDP, and VTP information about all users
- Layer 2 point-to-point tunneling to facilitate the automatic creation of EtherChannels
- Layer 2 protocol tunneling bypass feature to provide interoperability with third-party vendors
- IEEE 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network. These features are supported:
  - Multidomain authentication (MDA) to allow both a data device and a voice device, such as an IP phone (Cisco or non-Cisco), to independently authenticate on the same IEEE 802.1x-enabled enhanced EtherSwitch service module port
  - VLAN assignment for restricting IEEE 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to IEEE 802.1x ports
  - Voice VLAN to permit a Cisco IP Phone to access the voice VLAN regardless of the authorized or unauthorized state of the port
  - IP phone detection enhancement to detect and recognize a Cisco IP phone
  - Guest VLAN to provide limited services to non-IEEE 802.1x-compliant users
  - Restricted VLAN to provide limited services to users who are IEEE 802.1x compliant, but do not have the credentials to authenticate via the standard IEEE 802.1x processes
  - IEEE 802.1x accounting to track network usage
  - IEEE 802.1x with wake-on-LAN to allow dormant PCs to be powered on based on the receipt of a specific Ethernet frame
  - Voice aware IEEE 802.1x security to apply traffic violation actions only on the VLAN on which a security violation occurs
- MAC authentication bypass to authorize clients based on the client MAC address.

- Voice aware IEEE 802.1x and mac authentication bypass (MAB) security violation to shut down only the data VLAN on a port when a security violation occurs
- Network Admission Control (NAC) features:
  - NAC Layer 2 IEEE 802.1x validation of the antivirus condition or *posture* of endpoint systems or clients before granting the devices network access.

    For information about configuring NAC Layer 2 IEEE 802.1x validation, see *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
  - NAC Layer 2 IP validation of the posture of endpoint systems or clients before granting the devices network access.

    For information about configuring NAC Layer 2 IP validation, see *Network Admission Control Software Configuration Guide*.
  - IEEE 802.1x inaccessible authentication bypass.

    For information about configuring this feature, see *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
  - Authentication, authorization, and accounting (AAA) down policy for a NAC Layer 2 IP validation of a host if the AAA server is not available when the posture validation occurs.

    For information about this feature, see *Network Admission Control Software Configuration Guide*.
- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through AAA services
- Kerberos security system to authenticate requests for network resources by using a trusted third party (requires the cryptographic universal software image)
- Secure Socket Layer (SSL) Version 3.0 support for the HTTP 1.1 server authentication, encryption, and message integrity and HTTP client authentication to allow secure HTTP communications (requires the cryptographic universal software image)
- IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the enhanced EtherSwitch service module

QoS and CoS Features

These are the QoS and CoS features:

- Automatic QoS (auto-QoS) to simplify the deployment of existing QoS features by classifying traffic and configuring egress queues
- Classification
  - IP type-of-service/Differentiated Services Code Point (IP ToS/DSCP) and IEEE 802.1p CoS marking priorities on a per-port basis for protecting the performance of mission-critical applications
  - IP ToS/DSCP and IEEE 802.1p CoS marking based on flow-based packet classification (classification based on information in the MAC, IP, and TCP/UDP headers) for high-performance quality of service at the network edge, allowing for differentiated service levels for different types of network traffic and for prioritizing mission-critical traffic in the network

  - Trusted port states (CoS, DSCP, and IP precedence) within a QoS domain and with a port bordering another QoS domain
  - Trusted boundary for detecting the presence of a Cisco IP Phone, trusting the CoS value received, and ensuring port security
- Policing
  - Traffic-policing policies on the enhanced EtherSwitch service module port for managing how much of the port bandwidth should be allocated to a specific traffic flow
  - If you configure multiple class maps for a hierarchical policy map, each class map can be associated with its own port-level (second-level) policy map. Each second-level policy map can have a different policer.
  - Aggregate policing for policing traffic flows in aggregate to restrict specific applications or traffic flows to metered, predefined rates
- Out-of-Profile
  - Out-of-profile markdown for packets that exceed bandwidth utilization limits
- Ingress queueing and scheduling
  - Two configurable ingress queues for user traffic (one queue can be the priority queue)
  - Weighted tail drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
- Egress queues and scheduling
  - Four egress queues per port
  - WTD as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
  - SRR as the scheduling service for specifying the rate at which packets are dequeued to the egress interface (shaping or sharing is supported on egress queues). Shaped egress queues are guaranteed but limited to using a share of port bandwidth. Shared egress queues are also guaranteed a configured share of bandwidth, but can use more than the guarantee if other queues become empty and do not use their share of the bandwidth.
- Automatic quality of service (QoS) voice over IP (VoIP) enhancement for port -based trust of DSCP and priority queuing for egress traffic
- IPv6 port-based trust with dual IPv4 and IPv6 SDM templates

Layer 3 Features

These are the Layer 3 features:

Note Some features noted in this section are available only in the IP services feature set.

- HSRP Version 1 (HSRPv1) and HSRP Version 2 (HSRPv2) for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - OSPF (requires the IP services feature set)
  - Enhanced IGRP (EIGRP) (requires the IP services feature set)
  - Border Gateway Protocol (BGP) Version 4 (requires the IP services feature set)

- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Policy-based routing (PBR) for configuring defined policies for traffic flows
- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs (requires the IP services feature set)
- Fallback bridging for forwarding non-IP traffic between two or more VLANs (requires the IP services feature set)
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load-balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets
- Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode (requires the IP services feature set)
- Support for the SSM PIM protocol to optimize multicast applications, such as video
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains (requires the IP services feature set)
- Distance Vector Multicast Routing Protocol (DVMRP) tunneling for interconnecting two multicast-enabled networks across nonmulticast networks (requires the IP services feature set)
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- IPv6 default router preference (DRP) for improving the ability of a host to select an appropriate router
- Support for EIGRP IPv6, which utilizes IPv6 transport, communicates with IPv6 peers, and advertises IPv6 routes
- IP unicast reverse path forwarding (unicast RPF) for confirming source packet IP addresses.
- Nonstop forwarding (NSF) awareness to enable the Layer 3 enhanced EtherSwitch service module to continue forwarding packets from an NSF-capable neighboring router when the primary route processor (RP) is failing and the backup RP is taking over, or when the primary RP is manually reloaded for a nondisruptive software upgrade (requires the IP services feature set)
- The ability to exclude a port in a VLAN from the SVI line-state up or down calculation

Power over Ethernet Features

These are the Power over Ethernet (PoE) features:

- Ability to provide power to connected Cisco pre-standard and IEEE 802.3af-compliant powered devices from Power over Ethernet (PoE)-capable ports if the switch detects that there is no power on the circuit.
- Support for CDP with power consumption. The powered device notifies the enhanced EtherSwitch service module of the amount of power it is consuming. Layer 3 enhanced EtherSwitch service module also support PoE-Plus (20W per port).

- Support for Cisco intelligent power management. The powered device and the enhanced EtherSwitch service module negotiate through power-negotiation CDP messages for an agreed power-consumption level. The negotiation allows a high-power Cisco powered device to operate at its highest power mode.
- Automatic detection and power budgeting; the enhanced EtherSwitch service module maintains a power budget, monitors and tracks requests for power, and grants power only when it is available.
- Ability to monitor the real-time power consumption. On a per-PoE port basis, the enhanced EtherSwitch service module senses the total power consumption, polices the power usage, and reports the power usage.

Monitoring Features

These are the monitoring features:

- enhanced EtherSwitch service module LEDs that provide port- and enhanced EtherSwitch service module-level status on Catalyst 3560-E switches
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the enhanced EtherSwitch service module has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN
- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 traceroute to identify the physical path that a packet takes from a source device to a destination device
- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on 10/100 and 10/100/1000 copper Ethernet ports
- Online diagnostics to test the hardware functionality of the supervisor engine, modules, and enhanced EtherSwitch service module while the enhanced EtherSwitch service module is connected to a live network
- On-board failure logging (OBFL) to collect information about the enhanced EtherSwitch service module and the power supplies connected to it
- Enhanced object tracking (EOT) for HSRP to determine the proportion of hosts in a LAN by tracking the routing table state or to trigger the standby router failover
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down
- Flow-based enhanced EtherSwitch service module Port Analyzer (FSPAN) to define filters for capturing traffic for analysis

- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them though a policy

Default Settings After Initial Layer 2 and Layer 3 Enhanced EtherSwitch Service Module Configuration

The enhanced EtherSwitch service module is designed for plug-and-play operation, requiring only that you assign basic IP information to the enhanced EtherSwitch service module and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

Note For information about assigning an IP address by using the browser-based Express Setup program, see the getting started guide. For information about assigning an IP address by using the CLI-based setup program, see the hardware installation guide.

If you do not configure the enhanced EtherSwitch service module at all, the enhanced EtherSwitch service module operates with these default settings:

- Default enhanced EtherSwitch service module IP address, subnet mask, and default gateway is 0.0.0.0. For more information, see the Assigning the Switch IP Address and Default Gateway chapter and the Configuring DHCP Features and IP Source Guard chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- Default domain name is not configured. For more information, see the Assigning the Switch IP Address and Default Gateway chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- DHCP client is enabled, the DHCP server is enabled (only if the device acting as a DHCP server is configured and is enabled), and the DHCP relay agent is enabled (only if the device is acting as a DHCP relay agent is configured and is enabled). For more information, see the Assigning the Switch IP Address and Default Gateway chapter and the Configuring DHCP Features and IP Source Guard chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- No passwords are defined. For more information, see the Administering the Switch chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- System name and prompt is *Switch.* For more information, see the Administering the Switch chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- NTP is enabled. For more information, see the Administering the Switch chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- DNS is enabled. For more information, see the Administering the Switch chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*
- TACACS+ is disabled. For more information, see the Configuring Switch-Based Authentication chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- RADIUS is disabled. For more information, see the Configuring Switch-Based Authentication chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- The standard HTTP server and Secure Socket Layer (SSL) HTTPS server are both enabled. For more information, see the Configuring Switch-Based Authentication chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.

- IEEE 802.1x is disabled. For more information, see the Configuring IEEE 802.1x Port-Based Authentication chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- Port parameters
  - Operating mode is Layer 2 (switchport). For more information, see the Configuring Interface Characteristics chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
  - Interface speed and duplex mode is autonegotiate. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - Auto-MDIX is enabled. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
  - Flow control is off. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - PoE is autonegotiate. For more information, see the Configuring Interface Characteristics chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- No Smartports macros are defined. For more information, see the Configuring Smartports Macros chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- VLANs
  - Default VLAN is VLAN 1. For more information, see the Configuring VLANs chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - VLAN trunking setting is dynamic auto (DTP). For more information, see the Configuring VLANs chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - Trunk encapsulation is negotiate. For more information, see the Configuring VLANs chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - VTP mode is server. For more information, see the Configuring VTP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - VTP version is Version 1. For more information, see the Configuring VTP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - No private VLANs are configured. For more information, see the Configuring Private VLANs chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - Voice VLAN is disabled. For more information, see the Configuring Voice VLANs chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
  - IEEE 802.1Q tunneling and Layer 2 protocol tunneling are disabled. For more information, see Configuring IEEE 802.1Q and Layer 2 Protocol Tunneling chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- STP, PVST+ is enabled on VLAN 1. For more information, see the Configuring STP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- MSTP is disabled. For more information, see the Configuring MSTP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- Optional spanning-tree features are disabled. For more information, see the Configuring Optional Spanning-Tree Features chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*
- Flex Links are not configured. For more information, see the Configuring Flex Links and the MAC Address-Table Move Update Feature section in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide.*

- DHCP snooping is disabled. The DHCP snooping information option is enabled. For more information, see the Configuring DHCP Features and IP Source Guard chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- IP source guard is disabled. For more information, see the Configuring DHCP Features and IP Source Guard chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- Dynamic ARP inspection is disabled on all VLANs. For more information, see the Configuring Dynamic ARP Inspection chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- IGMP snooping is enabled. No IGMP filters are applied. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- IGMP throttling setting is deny. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- The IGMP snooping querier feature is disabled. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- MVR is disabled. For more information, see the Configuring IGMP Snooping and MVR chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- Port-based traffic
  - Broadcast, multicast, and unicast storm control is disabled. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
  - No protected ports are defined. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
  - Unicast and multicast traffic flooding is not blocked. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
  - No secure ports are configured. For more information, see the Configuring Port-Based Traffic Control chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- CDP is enabled. For more information, see the Configuring CDP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- UDLD is disabled. For more information, see the Configuring UDLD chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- SPAN and RSPAN are disabled. For more information, see the Configuring SPAN and RSPAN chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- RMON is disabled. For more information, see the Configuring RMON chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- Syslog messages are enabled and appear on the console. For more information, see the Configuring System Message Logging chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- SNMP is enabled (Version 1). For more information, see the Configuring SNMP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- No ACLs are configured. For more information, see the Configuring Network Security with ACLs chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- QoS is disabled. For more information, see the Configuring QoS chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.

- No EtherChannels are configured. For more information, see the Configuring EtherChannels and Link-State Tracking chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- IP unicast routing is disabled. For more information, see the Configuring IP Unicast Routing chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- No HSRP groups are configured. For more information, see the Configuring HSRP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- IP multicast routing is disabled on all interfaces. For more information, see the Configuring IP Multicast Routing chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- MSDP is disabled. For more information, see the Configuring MSDP chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.
- Fallback bridging is not configured. For more information, see the Configuring Fallback Bridging chapter in *Catalyst 3750-E and 3560-E Switch Software Configuration Guide*.

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*
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