Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch Interface Cards

This document provides configuration tasks for the 4-port Cisco HWIC-4ESW and the 9-port Cisco HWIC-D-9ESW EtherSwitch high speed WAN interface cards (HWICs) hardware feature supported on Cisco 1800 (modular), Cisco 2800, and Cisco 3800 series integrated services routers.

Cisco EtherSwitch HWICs are 10/100BaseT Layer 2 Ethernet switches with Layer 3 routing capability. (Layer 3 routing is forwarded to the host, and is not actually performed at the switch.). Traffic between different VLANs on a switch is routed through the router platform. Any one port on a Cisco EtherSwitch HWIC may be configured as a stacking port to link to another Cisco EtherSwitch HWIC or EtherSwitch network module in the same system. An optional power module can also be added to provide inline power for IP telephones. The HWIC-D-9ESW HWIC requires a double-wide card slot.

This hardware feature does not introduce any new or modified IOS commands.

Feature History for Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch Interface Cards

Release	Modification
12.3(8)T4	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

The following sections provide information about the Cisco EtherSwitch HWICs.

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

Prerequisites for EtherSwitch HWICs

The following are prerequisites to configuring EtherSwitch HWICs:

- Configuration of IP routing. (Refer to the *Cisco IOS IP Configuration Guide*.)
- Use of the Cisco IOS T Release, beginning with release 12.3(8)T4 or later for Cisco HWIC-4ESW and Cisco HWIC-D-9ESW support. (Refer to the Cisco IOS documentation.)

Restrictions for EtherSwitch HWICs

The following restrictions apply to the Cisco HWIC-4ESW and the Cisco HWIC-D-9ESW EtherSwitch HWICs.

- No more than two Ethernet Switch HWICs or network modules may be installed in a host router.

  Multiple Ethernet Switch HWICs or network modules installed in a host router will not act independently of each other. They must be stacked, as they will not work at all otherwise.
- The ports of a Cisco EtherSwitch HWIC must NOT be connected to the Fast Ethernet/Gigabit onboard ports of the router.
- There is no inline power on the ninth port (port 8) of the HWIC-D-9ESW card.
- There is no Auto MDIX support on the ninth port (port 8) of the HWIC-D-9ESW card when either **speed** or **duplex** is not set to **auto**.
- There is no support for online insertion/removal (OIR) of the EtherSwitch HWICs.
- When Ethernet Switches have been installed and configured in a host router, OIR of the CompactFlash memory card in the router must not occur. OIR of the CompactFlash memory card will compromise the configuration of the Ethernet Switches.
- VTP pruning is not supported.
- There is a limit of 200 secure MAC addresses per module that can be supported by an EtherSwitch HWIC.

Information About EtherSwitch HWICs

To configure the Cisco HWIC-4ESW and HWIC-D-9ESW EtherSwitch HWICs, you should understand the following concepts:

- Switched Port Analyzer, page 4
- IGMP Snooping, page 4
- Storm Control, page 4
- Intrachassis Stacking, page 4
- Fallback Bridging, page 4

VLANs

For information on the concept of VLANs, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1047027

Inline Power for Cisco IP Phones

For information on the concept of inline power for Cisco IP phones, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1048439

Layer 2 Ethernet Switching

For information on the concept of Layer 2 Ethernet Switching, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1048478

802.1x Authentication

For Information on the concept of 802.1x Authentication, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1051006

Spanning Tree Protocol

For Information on the concept of Spanning Tree Protocol, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1048458

Cisco Discovery Protocol

For Information on the concept of the Cisco Discovery Protocol, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1048498

Switched Port Analyzer

For Information on the concept of Switched Port Analyzer, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1053663

IGMP Snooping

For Information on the concept of IGMP Snooping, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1053727

Storm Control

For Information on the concept of Storm Control, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1051018

Intrachassis Stacking

For Information on the concept of Intrachassis Stacking, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1051061

Fallback Bridging

For Information on the concept of Fallback Bridging, refer to the material at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1054833

How to Configure EtherSwitch HWICs

See the following sections for configuration tasks for the EtherSwitch HWICs.

- Configuring VLANs, page 5
- Configuring VLAN Trunking Protocol, page 9
- Configuring Layer 2 Interfaces, page 11
- Configuring 802.1x Authentication, page 18
- Configuring Spanning Tree, page 26
- Configuring MAC Table Manipulation, page 32
- Configuring Cisco Discovery Protocol, page 34
- Configuring the Switched Port Analyzer (SPAN), page 36
- Configuring Power Management on the Interface, page 37
- Configuring IP Multicast Layer 3 Switching, page 39
- Configuring IGMP Snooping, page 42
- Configuring Per-Port Storm-Control, page 46
- Configuring Stacking, page 47
- Configuring Fallback Bridging, page 48
- Configuring Separate Voice and Data Subnets, page 59
- Managing the EtherSwitch HWIC, page 61

Configuring VLANs

This section describes how to configure VLANs on the switch, and contains the following sections:

- Adding VLAN Instances, page 5
- Deleting a VLAN Instance from the Database, page 8

Adding VLAN Instances

A total of 15 VLANs are supported by an EtherSwitch HWIC.

Beginning in privileged EXEC mode, follow these steps to configure a Fast Ethernet interface as Layer 2 access:

SUMMARY STEPS

1. **`vlan database`**
2. **`vlan`** *`vlan_id`*
3. **`exit`**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#`**`vlan database`**	Enters VLAN configuration mode.
Step 2	`Router(vlan)#`**`vlan`** *`vlan_id`*	Adds an Ethernet VLAN.
Step 3	`Router(vlan)#`**`exit`**	Updates the VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode.

Verifying the VLAN Configuration

You can verify the VLAN configuration in VLAN database mode.

Use the **show** command in VLAN database mode to verify the VLAN configuration, as shown below:

```
Router(vlan)#show
  VLAN ISL Id: 1
  Name: default
  Media Type: Ethernet
  VLAN 802.10 Id: 100001
  State: Operational
  MTU: 1500
  Translational Bridged VLAN: 1002
  Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
  Name: VLAN0002
  Media Type: Ethernet
  VLAN 802.10 Id: 100002
  State: Operational
  MTU: 1500

  VLAN ISL Id: 3
  Name: Red_VLAN
  Media Type: Ethernet
  VLAN 802.10 Id: 100003
  State: Operational
  MTU: 1500

  VLAN ISL Id: 1002
  Name: fddi-default
  Media Type: FDDI
  VLAN 802.10 Id: 101002
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1003

  VLAN ISL Id: 1003
  Name: token-ring-default
  Media Type: Token Ring
  VLAN 802.10 Id: 101003
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Ring Number: 0
  Bridge Number: 1
  Parent VLAN: 1005
  Maximum ARE Hop Count: 7
  Maximum STE Hop Count: 7
  Backup CRF Mode: Disabled
  Translational Bridged VLAN: 1
  Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
   Name: fddinet-default
  Media Type: FDDI Net
  VLAN 802.10 Id: 101004
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Bridge Number: 1
  STP Type: IBM

  VLAN ISL Id: 1005
  Name: trnet-default
  Media Type: Token Ring Net
  VLAN 802.10 Id: 101005
  State: Operational
  MTU: 1500
  Bridge Type: SRB
  Bridge Number: 1
  STP Type: IBM

router(vlan)# exit
APPLY completed.
Exiting....
router#
router#
```

Enter the **show vlan-switch** command in EXEC mode using the Cisco IOS CLI to verify the VLAN configuration, as shown below:

```
router#show vlan-switch
VLAN Name                             Status    Ports
---- -------------------------------- --------- ----------------------------------
1    default                          active    Fa0/1/1, Fa0/1/2, Fa0/1/3, Fa0/1/4
                                                Fa0/1/5, Fa0/1/6, Fa0/1/7, Fa0/1/8
                                                Fa0/3/0, Fa0/3/2, Fa0/3/3, Fa0/3/4
                                                Fa0/3/5, Fa0/3/6, Fa0/3/7, Fa0/3/8
2    VLAN0002                         active    Fa0/1/0
3    Red_VLAN                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
router#
```

Deleting a VLAN Instance from the Database

You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.

Beginning in privileged EXEC mode, follow these steps to delete a VLAN from the database:

SUMMARY STEPS

1. **vlan database**
2. **no vlan** *vlan_id*
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	Router#**vlan database**	Enters VLAN configuration mode.
Step 2	Router(vlan)#**no vlan** *vlan_id*	Deletes the VLAN.
Step 3	Router(vlan)#**exit**	Updates the VLAN database, propagates it throughout the administrative domain, and returns to privileged EXEC mode.

Verifying VLAN Deletion

You can verify that a VLAN has been deleted from the switch in VLAN database mode.

Use the **show** command in VLAN database mode to verify that a VLAN has been deleted from the switch, as shown in the following output example:

```
Router(vlan)#show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003
<output truncated>

Router(vlan)#
```

Enter the **show vlan-switch brief** command in EXEC mode, using the Cisco IOS CLI to verify that a VLAN has been deleted from the switch, as shown in the following output example:

```
Router#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1/0, Fa0/1/1, Fa0/1/2
                                                Fa0/1/3, Fa0/1/4, Fa0/1/5
                                                Fa0/1/6, Fa0/1/7, Fa0/1/8
300  VLAN0300                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Router#
```

Configuring VLAN Trunking Protocol

This section describes how to configure the VLAN Trunking Protocol (VTP) on an EtherSwitch HWIC, and contains the following sections:

- Configuring a VTP Server, page 9
- Configuring a VTP Client, page 10
- Disabling VTP (VTP Transparent Mode), page 10
- Verifying VTP, page 11

Note VTP pruning is not supported by EtherSwitch HWICs.

Configuring a VTP Server

When a switch is in VTP server mode, you can change the VLAN configuration and have it propagate throughout the network.

Beginning in privileged EXEC mode, follow these steps to configure the switch as a VTP server.

SUMMARY STEPS

1. **vlan database**
2. **vtp server**
3. **vtp domain** *domain_name*
4. **vtp password** *password_value*
5. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	`Router# vlan database`	Enters VLAN configuration mode.
Step 2	`Router(vlan)# vtp server`	Configures the switch as a VTP server.

	Command	Purpose
Step 3	`Router(vlan)# vtp domain domain_name`	Defines the VTP domain name, which can be up to 32 characters long.
Step 4	`Router(vlan)# vtp password password_value`	(Optional) Sets a password, which can be from 8 to 64 characters long, for the VTP domain.
Step 5	`Router(vlan)# exit`	Exits VLAN configuration mode.

Configuring a VTP Client

When a switch is in VTP client mode, you cannot change the VLAN configuration on the switch. The client switch receives VTP updates from a VTP server in the management domain and modifies its configuration accordingly.

Beginning in privileged EXEC mode, follow these steps to configure the switch as a VTP client.

SUMMARY STEPS

1. **vlan database**
2. **vtp client**
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	`Router# vlan database`	Enters VLAN configuration mode.
Step 2	`Router(vlan)# vtp client`	Configures the switch as a VTP client.
Step 3	`Router(vlan)# exit`	Exits VLAN configuration mode.

Disabling VTP (VTP Transparent Mode)

When you configure the switch as VTP transparent, you disable VTP on the switch. A VTP transparent switch does not send VTP updates and does not act on VTP updates received from other switches.

Beginning in privileged EXEC mode, follow these steps to disable VTP on the switch.

SUMMARY STEPS

1. **vlan database**
2. **vtp transparent**
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	`Router# vlan database`	Enters VLAN configuration mode.
Step 2	`Router(vlan)# vtp transparent`	Configures VTP transparent mode.
Step 3	`Router(vlan)# exit`	Exits VLAN configuration mode.

Verifying VTP

Use the **show vtp status** to verify VTP status:

```
Router# show vtp status

VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 256
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xBF 0x86 0x94 0x45 0xFC 0xDF 0xB5 0x70
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 1.3.214.25 on interface Fa0/0 (first interface found)
Router#
```

Configuring Layer 2 Interfaces

This section provides the following configuration information:

- Configuring a Range of Interfaces, page 12 (required)
- Defining a Range Macro, page 12 (optional)
- Configuring Layer 2 Optional Interface Features, page 13 (optional)

Configuring a Range of Interfaces

Use the **interface range** command in global configuration mode to configure a range of interfaces.

<table>
<tr><th>Command</th><th>Purpose</th></tr>
<tr><td>Router(config)#<b>interface range</b> {<b>macro</b> <i>macro_name</i> | <b>FastEthernet</b> <i>interface-id</i> [<b>-</b> <i>interface-id</i>] | <b>vlan</b> vlan_ID} [<b>,</b> <b>FastEthernet</b> <i>interface-id</i> [- <i>interface-id</i>] | <b>vlan</b> <i>vlan_ID</i>]</td><td>Select the range of interfaces to be configured.
• The space before the dash is required. For example, the command <b>interface range fastethernet</b> 0/&lt;<i>slot</i>&gt;/<b>0 -</b> 0/&lt;<i>slot</i>&gt;/<b>3</b> is valid; the command <b>interface range fastethernet</b> 0/&lt;<i>slot</i>&gt;/<b>0-</b>0/&lt;<i>slot</i>&gt;<b>/3</b> is not valid.
• You can enter one macro or up to five comma-separated ranges.
• Comma-separated ranges can include both VLANs and physical interfaces.
• You are not required to enter spaces before or after the comma.
• The <b>interface range</b> command only supports VLAN interfaces that are configured with the <b>interface vlan</b> command.</td></tr>
</table>

Defining a Range Macro

Use the **define interface-range** command in global configuration mode to define an interface range macro:

<table>
<tr><th>Command</th><th>Purpose</th></tr>
<tr><td>Router(config)#<b>define interface-range</b> <i>macro_name</i> {<b>FastEthernet</b> <i>interface-id</i> [- <i>interface-id</i>] | {<b>vlan</b> <i>vlan_ID - vlan_ID</i>} | [<b>,</b> <b>FastEthernet</b> <i>interface-id</i> [- <i>interface-id</i>]</td><td>Define the interface-range macro and save it in NVRAM.</td></tr>
</table>

Verifying Configuration of an Interface Range Macro

Use the **show running-configuration** command to show the defined interface-range macro configuration, as shown below:

```
Router#show running-configuration | include define
define interface-range first_three FastEthernet0/1/0 - 2
```

Configuring Layer 2 Optional Interface Features

Interface Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- If both ends of the line support autonegotiation, Cisco highly recommends the default auto negotiation settings.
- If one interface supports auto negotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- Both ends of the line need to be configured to the same setting. For example, both hard-set or both auto-negotiate. Mismatched settings are not supported.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

Configuring the Interface Speed

Beginning in global configuration mode, follow these steps to set the interface speed.

SUMMARY STEPS

1. **`interface fastethernet`** *`interface-id`*
2. **`speed`** `[`**`10`** `|` **`100`** `|` **`auto`**`]`

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#`**`interface fastethernet`** *`interface-id`*	Selects the interface to be configured.
Step 2	`Router(config-if)#`**`speed`** `[`**`10`** `|` **`100`** `|` **`auto`**`]`	Sets the interface speed of the interface.

Note If you set the interface speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are auto negotiated.

Configuring the Interface Duplex Mode

Beginning in global configuration mode, follow these steps to set the duplex mode of a Fast Ethernet interface.

SUMMARY STEPS

1. **interface fastethernet** *interface-id*
2. **duplex [auto | full | half]**

DETAILED STEPS

	Command	Purpose
Step 1	Router(config)#**interface fastethernet** *interface-id*	Selects the interface to be configured.
Step 2	Router(config-if)#**duplex [auto | full | half]**	Sets the duplex mode of the interface.

Note If you set the port speed to auto on a 10/100-Mbps Ethernet interface, both speed and duplex are auto negotiated. You cannot change the duplex mode of auto negotiation interfaces.

The following example shows how to set the interface duplex mode to auto on Fast Ethernet interface 3:

```
Router(config)#interface fastethernet 0/1/0
router(config-if)#speed 100
Router(config-if)#duplex auto
Router(config-if)#end
```

Verifying Interface Speed and Duplex Mode Configuration

Use the **show interfaces** command to verify the interface speed and duplex mode configuration for an interface, as shown in the following output example:

```
Router#show interfaces fastethernet 0/1/0

FastEthernet0/1/0 is up, line protocol is up
 Hardware is Fast Ethernet, address is 000f.f70a.f272 (bia 000f.f70a.f272)
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
   reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Auto-duplex, Auto-speed
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:11, output never, output hang never
 Last clearing of "show interface" counters never
 Queueing strategy: fifo
 Output queue 0/40, (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
   4 packets input, 1073 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 input packets with dribble condition detected
   6 packets output, 664 bytes, 0 underruns(0/0/0)
   0 output errors, 0 collisions, 3 interface resets
```

```
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
Router#
```

Configuring a Description for an Interface

You can add a description of an interface to help you remember its function. The description appears in the output of the following commands: **show configuration**, **show running-config**, and **show interfaces**.

Use the **description** command, in interface configuration mode, to add a description for an interface:

Command	Purpose
`Router(config-if)#`**`description`** *`string`*	Adds a description for an interface.

Configuring a Fast Ethernet Interface as a Layer 2 Trunk

Beginning in global configuration mode, follow these steps to configure a Fast Ethernet interface as a Layer 2 trunk.

SUMMARY STEPS

1. **`interface fastethernet`** *`interface-id`*
2. **`shutdown`**
3. **`switchport mode trunk`**
4. **`switchport trunk native vlan`** *`vlan-num`*
5. **`switchport trunk allowed vlan`** `{`**`add`** `|` **`except`** `|` **`none`** `|` **`remove`**`}` *`vlan1`*`[,`*`vlan`*`[,`*`vlan`*`[,...]]`
6. **`no shutdown`**
7. **`end`**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#` **`interface fastethernet`** *`interface-id`*	Selects the interface to configure.
Step 2	`Router(config-if)#` **`shutdown`**	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3	`Router(config-if)#` **`switchport mode trunk`**	Configures the interface as a Layer 2 trunk. **Note** Encapsulation is always dot1q.
Step 4	`Router(config-if)#` **`switchport trunk native vlan`** *`vlan-num`*	(Optional) For 802.1Q trunks, specifies the native VLAN.
Step 5	`Router(config-if)#` **`switchport trunk allowed vlan`** `{`**`add`** `|` **`except`** `|` **`none`** `|` **`remove`**`}` *`vlan1`*`[,`*`vlan`*`[,`*`vlan`*`[,...]]`	(Optional) Configures the list of VLANs allowed on the trunk. All VLANs are allowed by default. You cannot remove any of the default VLANs from a trunk.

	Command	Purpose
Step 6	`Router(config-if)# no shutdown`	Activates the interface. (Required only if you shut down the interface.)
Step 7	`Router(config-if)# end`	Exits configuration mode.

Note Ports do not support Dynamic Trunk Protocol (DTP). Ensure that the neighboring switch is set to a mode that will not send DTP.

Verifying a Fast Ethernet Interface as a Layer 2 Trunk

Use the following **show** commands to verify the configuration of a Fast Ethernet interface as a Layer 2 trunk:

```
router#show running-config interfaces fastEthernet 0/3/1
Building configuration...
Current configuration: 71 bytes
!
interface FastEthernet0/3/1
  switchport mode trunk
  no ip address
end
router#

router#show interfaces trunk
Port  Mode  Encapsulation  Status  Native vlan
Fa0/3/1  on     802.1q      trunking     1

Port  Vlans allowed on trunk
Fa0/3/1    1-1005

Port  Vlans allowed and active in management domain
Fa0/3/1    1

Port  Vlans in spanning tree forwarding state and not pruned
Fa0/3/1    1

router#
```

Configuring a Fast Ethernet Interface as Layer 2 Access

Beginning in global configuration mode, follow these steps to configure a Fast Ethernet interface as Layer 2 access.

SUMMARY STEPS

1. **interface fastethernet** *interface-id*
2. **shutdown**
3. **switchport mode access**
4. **switchport access vlan** *vlan_num*
5. **no shutdown**
6. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#`**`interface fastethernet`** *`interface-id`*	Selects the interface to configure.
Step 2	`Router(config-if)#`**`shutdown`**	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete.
Step 3	`Router(config-if)#`**`switchport mode access`**	Configures the interface as a Layer 2 access.
Step 4	`Router(config-if)#`**`switchport access vlan`** *`vlan_num`*	For access ports, specifies the access vlan.
Step 5	`Router(config-if)#`**`no shutdown`**	Activates the interface. (Required only if you shut down the interface.)
Step 6	`Router(config-if)#`**`end`**	Exits configuration mode.

Verifying a Fast Ethernet Interface as Layer 2 Access

Use the **show running-config interface** command to verify the running configuration of the interface, as shown below:

```
Router#show running-config interface fastethernet 0/1/2
Building configuration...
Current configuration: 76 bytes
!
interface FastEthernet0/1/2
  switchport access vlan 3
  no ip address
end
```

Use the **show interfaces** command to verify the switchport configuration of the interface, as shown below:

```
Router#show interfaces f0/1/0 switchport
Name: Fa0/1/0
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Disabled
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
router#
```

Configuring 802.1x Authentication

This section describes how to configure 802.1x port-based authentication on an EtherSwitch HWIC:

Understanding the Default 802.1x Configuration

Table 1 shows the default 802.1x configuration.

Table 1 Default 802.1x Configuration

Feature	Default Setting
Authentication, authorization, and accounting (AAA)	Disabled.
RADIUS server • IP address • UDP authentication port • Key	 • None specified. • 1645. • None specified.
Per-interface 802.1x enable state	Disabled (force-authorized). The port transmits and receives normal traffic without 802.1x-based authentication of the client.
Periodic reauthentication	Disabled.
Number of seconds between reauthentication attempts	3600 seconds.
Quiet period	60 seconds (number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client).
Retransmission time	30 seconds (number of seconds that the switch should wait for a response to an EAP request/identity frame from the client before retransmitting the request).
Maximum retransmission number	2 times (number of times that the switch will send an EAP-request/identity frame before restarting the authentication process).
Multiple host support	Disabled.

Table 1 Default 802.1x Configuration (continued)

Feature	Default Setting
Client timeout period	30 seconds (when relaying a request from the authentication server to the client, the amount of time the switch waits for a response before retransmitting the request to the client). This setting is not configurable.
Authentication server timeout period	30 seconds (when relaying a response from the client to the authentication server, the amount of time the switch waits for a reply before retransmitting the response to the server). This setting is not configurable.

802.1x Configuration Guidelines

These are the 802.1x authentication configuration guidelines:

- When the 802.1x protocol is enabled, ports are authenticated before any other Layer 2 feature is enabled.
- The 802.1x protocol is supported on Layer 2 static-access ports, but it is not supported on these port types:
  - Trunk port—If you try to enable 802.1x on a trunk port, an error message appears, and 802.1x is not enabled. If you try to change the mode of an 802.1x-enabled port to trunk, the port mode is not changed.
  - Switch Port Analyzer (SPAN) destination port—You can enable 802.1x on a port that is a SPAN destination port; however, 802.1x is disabled until the port is removed as a SPAN destination. You can enable 802.1x on a SPAN source port.

Enabling 802.1x Authentication

To enable 802.1x port-based authentication, you must enable AAA and specify the authentication method list. A method list describes the sequence and authentication methods to be queried to authenticate a user.

The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle, the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure 802.1x port-based authentication. This procedure is required.

SUMMARY STEPS

1. **`configure terminal`**
2. **`configure terminal`**
3. **`aaa authentication`** `dot1x {default |` *`listname`*`}` *`method1`* `[`*`method2`*`...]`
4. **`interface`** *`interface-id`*
5. **`dot1x port-control auto`**
6. **`end`**

7. **show dot1x**
8. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**aaa new-model**	Enables AAA.
Step 3	**aaa authentication** dot1x {default | *listname*} *method1* [*method2*...]	Creates an 802.1x authentication method list. To create a default list that is used when a named list is *not* specified in the **authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. Enter at least one of these keywords: • **group radius**—Use the list of all RADIUS servers for authentication. • **none**—Use no authentication. The client is automatically authenticated without the switch using the information supplied by the client.
Step 4	**interface** *interface-id*	Enters interface configuration mode, and specify the interface to be enabled for 802.1x authentication.
Step 5	**dot1x port-control auto**	Enables 802.1x on the interface. For feature interaction information with trunk, dynamic, dynamic-access, EtherChannel, secure, and SPAN ports see the "802.1x Configuration Guidelines" section on page 19.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**show dot1x**	Verifies your entries. Check the Status column in the 802.1x Port Summary section of the display. An *enabled* status means the port-control value is set either to **auto** or to **force-unauthorized**.
Step 8	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable 802.1x AAA authentication, use the **no aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...] global configuration command. To disable 802.1x, use the **dot1x port-control force-authorized** or the **no dot1x port-control** interface configuration command.

Configuring the Switch-to-RADIUS-Server Communication

RADIUS security servers are identified by their host name or IP address, host name and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, which enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, authentication—the second host entry configured acts as the fail-over backup to the first one. The RADIUS host entries are tried in the order that they were configured.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch. This procedure is required.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**radius-server host** {*hostname* | *ip-address*} **auth-port** *port-number* **key** *string*	Configures the RADIUS server parameters on the switch. For *hostname* | *ip-address*, specify the host name or IP address of the remote RADIUS server. For **auth-port** *port-number*, specify the UDP destination port for authentication requests. The default is 1645. For **key** *string*, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server. The key is a text string that must match the encryption key used on the RADIUS server. **Note** Always configure the key as the last item in the **radius-server host** command syntax because leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks are part of the key. This key must match the encryption used on the RADIUS daemon. If you want to use multiple RADIUS servers, repeat this command.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To delete the specified RADIUS server, use the **no radius-server host** {*hostname* | *ip-address*} global configuration command.

You can globally configure the timeout, retransmission, and encryption key values for all RADIUS servers by using the **radius-server host** global configuration command. If you want to configure these options on a per-server basis, use the **radius-server timeout**, **radius-server retransmit**, and the **radius-server key** global configuration commands.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, refer to the RADIUS server documentation.

Enabling Periodic Reauthentication

You can enable periodic 802.1x client reauthentication and specify how often it occurs. If you do not specify a time period before enabling reauthentication, the number of seconds between reauthentication attempts is 3600 seconds.

Automatic 802.1x client reauthentication is a global setting and cannot be set for clients connected to individual ports.

Beginning in privileged EXEC mode, follow these steps to enable periodic reauthentication of the client and to configure the number of seconds between reauthentication attempts:

SUMMARY STEPS

1. **configure terminal**
2. **dot1x re-authentication**
3. **dot1x timeout re-authperiod** *seconds*
4. **end**
5. **show dot1x**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**dot1x re-authentication**	Enables periodic reauthentication of the client, which is disabled by default.
Step 3	**dot1x timeout re-authperiod** *seconds*	Sets the number of seconds between reauthentication attempts. The range is 1 to 4294967295; the default is 3600 seconds. This command affects the behavior of the switch only if periodic reauthentication is enabled.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show dot1x**	Verifies your entries.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable periodic reauthentication, use the **no dot1x re-authentication** global configuration command. To return to the default number of seconds between reauthentication attempts, use the **no dot1x timeout re-authperiod** global configuration command.

Changing the Quiet Period

When the switch cannot authenticate the client, the switch remains idle for a set period of time, and then tries again. The idle time is determined by the quiet-period value. A failed authentication of the client might occur because the client provided an invalid password. You can provide a faster response time to the user by entering smaller number than the default.

Beginning in privileged EXEC mode, follow these steps to change the quiet period:

SUMMARY STEPS

1. **configure terminal**
2. **dot1x timeout quiet-period** *seconds*
3. **end**
4. **show dot1x**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**dot1x timeout quiet-period** *seconds*	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 0 to 65535 seconds; the default is 60.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show dot1x**	Verifies your entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To return to the default quiet time, use the **no dot1x timeout quiet-period** global configuration command.

Changing the Switch-to-Client Retransmission Time

The client responds to the EAP-request/identity frame from the switch with an EAP-response/identity frame. If the switch does not receive this response, it waits a set period of time (known as the retransmission time), and then retransmits the frame.

Note You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to change the amount of time that the switch waits for client notification:

SUMMARY STEPS

1. **configure terminal**
2. **dot1x timeout tx-period** *seconds*
3. **end**
4. **show dot1x**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`dot1x timeout tx-period`** *`seconds`*	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535 seconds; the default is 30.
Step 3	**`end`**	Returns to privileged EXEC mode.
Step 4	**`show dot1x`**	Verifies your entries.
Step 5	**`copy running-config startup-config`**	(Optional) Saves your entries in the configuration file.

To return to the default retransmission time, use the **no dot1x timeout tx-period** global configuration command.

Setting the Switch-to-Client Frame-Retransmission Number

In addition to changing the switch-to-client retransmission time, you can change the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

Note You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Beginning in privileged EXEC mode, follow these steps to set the switch-to-client frame-retransmission number:

SUMMARY STEPS

1. **`configure terminal`**
2. **`dot1x max-req`** *`count`*
3. **`end`**
4. **`show dot1x`**
5. **`copy running-config startup-config`**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`dot1x max-req`** *`count`*	Sets the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.
Step 3	**`end`**	Returns to privileged EXEC mode.

	Command	Purpose
Step 4	**`show dot1x`**	Verifies your entries.
Step 5	**`copy running-config startup-config`**	(Optional) Saves your entries in the configuration file.

To return to the default retransmission number, use the **no dot1x max-req** global configuration command.

Enabling Multiple Hosts

You can attach multiple hosts to a single 802.1x-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails, and an EAPOL-logoff message is received), all attached clients are denied access to the network.

Beginning in privileged EXEC mode, follow these steps to allow multiple hosts (clients) on an 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**.

SUMMARY STEPS

1. **`configure terminal`**
2. **`interface`** *`interface-id`*
3. **`dot1x multiple-hosts`**
4. **`end`**
5. **`show dot1x interface`** *`interface-id`*
6. **`copy running-config startup-config`**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`interface`** *`interface-id`*	Enters interface configuration mode, and specify the interface to which multiple hosts are indirectly attached.
Step 3	**`dot1x multiple-hosts`**	Allows multiple hosts (clients) on an 802.1x-authorized port. Make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified interface.
Step 4	**`end`**	Returns to privileged EXEC mode.
Step 5	**`show dot1x interface`** *`interface-id`*	Verifies your entries.
Step 6	**`copy running-config startup-config`**	(Optional) Saves your entries in the configuration file.

To disable multiple hosts on the port, use the **no dot1x multiple-hosts** interface configuration command.

Resetting the 802.1x Configuration to the Default Values

You can reset the 802.1x configuration to the default values with a single command.

Beginning in privileged EXEC mode, follow these steps to reset the 802.1x configuration to the default values:

SUMMARY STEPS

1. **configure terminal**
2. **dot1x default**
3. **end**
4. **show dot1x**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**dot1x default**	Resets the configurable 802.1x parameters to the default values.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show dot1x**	Verifies your entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Displaying 802.1x Statistics and Status

To display 802.1x statistics for all interfaces, use the **show dot1x statistics** privileged EXEC command. To display 802.1x statistics for a specific interface, use the **show dot1x statistics interface** *interface-id* privileged EXEC command.

To display the 802.1x administrative and operational status for the switch, use the **show dot1x** privileged EXEC command. To display the 802.1x administrative and operational status for a specific interface, use the **show dot1x interface** *interface-id* privileged EXEC command.

Configuring Spanning Tree

- Enabling Spanning Tree, page 27
- Configuring Spanning Tree Port Priority, page 27
- Configuring Spanning Tree Port Cost, page 28
- Configuring the Bridge Priority of a VLAN, page 30
- Configuring the Hello Time, page 30
- Configuring the Forward-Delay Time for a VLAN, page 31
- Configuring the Maximum Aging Time for a VLAN, page 31
- Disabling Spanning Tree, page 32

Enabling Spanning Tree

You can enable spanning tree on a per-VLAN basis. The switch maintains a separate instance of spanning tree for each VLAN (except on VLANs on which you disable spanning tree).

To enable spanning tree on a per-VLAN basis, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`spanning-tree vlan`** *`vlan_ID`*	Enables spanning tree on a per-VLAN basis.

Verifying Spanning Tree

Use the **show spanning-tree vlan** to verify spanning tree configuration, as illustrated below:

```
Router# show spanning-tree vlan 200
 VLAN200 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0050.3e8d.6401
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 16384, address 0060.704c.7000
  Root port is 264 (FastEthernet0/1/8), cost of root path is 38
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 01:53:48 ago
  Times:  hold 1, topology change 24, notification 2
          hello 2, max age 14, forward delay 10
  Timers: hello 0, topology change 0, notification 0


 Port 264 (FastEthernet0/1/8) of VLAN200 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 129.9.
   Designated root has priority 16384, address 0060.704c.7000
   Designated bridge has priority 32768, address 00e0.4fac.b000
   Designated port id is 128.2, designated path cost 19
   Timers: message age 3, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 3, received 3417

Router#
```

Configuring Spanning Tree Port Priority

Beginning in global configuration mode, follow these steps to configure the spanning tree port priority of an interface.

SUMMARY STEPS

1. **interface** {{**ethernet** | **fastethernet**} *interface-id*
2. [**no**] **spanning-tree port-priority** *port_priority*
3. [**no**] **spanning-tree vlan** *vlan_ID* **port-priority** *port_priority*
4. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#` **`interface`** `{{`**`ethernet`** `|` **`fastethernet`**`}` *`interface-id`*	Selects an interface to configure.
Step 2	`Router(config-if)# [`**`no`**`]` **`spanning-tree port-priority`** *`port_priority`*	Configures the port priority for an interface. The of port_priority value can be from 4 to 252 in increments of 4. Use the **no** form of this command to restore the defaults.
Step 3	`Router(config-if)# [`**`no`**`]` **`spanning-tree vlan`** *`vlan_ID`* **`port-priority`** *`port_priority`*	Configures the VLAN port priority for an interface. The port_priority value can be from 4 to 252 in increments of 4. Use the **no** form of this command to restore the defaults.
Step 4	`Router(config-if)#` **`end`**	Exits configuration mode.

Verifying Spanning Tree Port Priority

Use the **show spanning-tree interface** to verify spanning-tree interface and the spanning-tree port priority configuration, as illustrated below:

```
Router# show spanning-tree interface fastethernet 0/1/6

 Port 264 (FastEthernet0/1/6) of VLAN200 is forwarding
   Port path cost 19, Port priority 100, Port Identifier 129.8.
   Designated root has priority 32768, address 0010.0d40.34c7
   Designated bridge has priority 32768, address 0010.0d40.34c7
   Designated port id is 128.1, designated path cost 0
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 0, received 13513
Router#
```

Configuring Spanning Tree Port Cost

Beginning in global configuration mode, follow these steps to configure the spanning tree port cost of an interface.

SUMMARY STEPS

1. **`interface`** `{{`**`ethernet`** `|` **`fastethernet`**`}` *`interface-id`*
2. `[`**`no`**`]` **`spanning-tree cost`** *`port_cost`*
3. `[`**`no`**`]` **`spanning-tree vlan`** *`vlan_ID`* **`cost`** *`port_cost`*
4. **`end`**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#` **`interface`** `{{`**`ethernet`** `|` **`fastethernet`**`}` *`interface-id`*	Selects an interface to configure.
Step 2	`Router(config-if)# [`**`no`**`]` **`spanning-tree cost`** *`port_cost`*	Configures the port cost for an interface. The value of port_cost can be from 1 to 200,000,000 (1 to 65,535 in Cisco IOS Releases 12.1(2)E and earlier). Use the **no** form of this command to restore the defaults.
Step 3	`Router(config-if)# [`**`no`**`]` **`spanning-tree vlan`** *`vlan_ID`* **`cost`** *`port_cost`*	Configures the VLAN port cost for an interface. The value port_cost can be from 1 to 65,535. Use the **no** form of this command to restore the defaults.
Step 4	`Router(config-if)#` **`end`**	Exits configuration mode.

Calculating Port Cost

Port cost value calculations are based on the bandwidth of the port. There are two classes of values. Short (16-bit) values are specified by the IEEE 802.1D specification, and range in value from 1 to 65535. Long (32-bit) values are specified by the IEEE 802.1t specification, and range in value from1 to 200,000,000.

Assigning Short Port Cost Values

You can manually assign port costs in the range of 1 to 65535. Default cost values are as follows.

Port Speed	Default Cost Value
10 Mbps	100
100 Mbps	19

Assigning Long Port Cost Values

You can manually assign port costs in the range of 1 to 200,000,000. Recommended cost values are as follows.

Port Speed	Recommended Value	Recommended Range
10 Mbps	2,000,000	200,000 to 20,000,000
100 Mbps	200,000	20,000 to 2,000,000

Verifying Spanning Tree Port Cost

Use the **show spanning-tree vlan** to verify the spanning-tree port cost configuration.

```
Router# show spanning-tree vlan 200

Port 264 (FastEthernet0/1/8) of VLAN200 is forwarding
Port path cost 17, Port priority 64, Port Identifier 129.8.
   Designated root has priority 32768, address 0010.0d40.34c7
   Designated bridge has priority 32768, address 0010.0d40.34c7
   Designated port id is 128.1, designated path cost 0
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   BPDU: sent 0, received 13513
Router#
```

Configuring the Bridge Priority of a VLAN

To configure the spanning tree bridge priority of a VLAN, use the following command in global configuration mode:

Command	Purpose
`Router(config)# [`**`no`**`]` **`spanning-tree vlan`** *`vlan_ID`* **`priority`** *`bridge_priority`*	Configures the bridge priority of a VLAN. The bridge_priority value can be from 1 to 65535. Use the **no** form of this command to restore the defaults.

Caution Exercise care when using this command. For most situations **spanning-tree vlan vlan_ID root primary** and the **spanning-tree vlan vlan_ID root secondary** are the preferred commands to modify the bridge priority.

Verifying the Bridge Priority of a VLAN

Use the **show spanning-tree vlan bridge** command to verify the bridge priority, as illustrated below:

```
Router# show spanning-tree vlan 200 bridge brief
                                      Hello Max Fwd
Vlan                   Bridge ID      Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          33792 0050.3e8d.64c8    2   20    15  ieee
Router#
```

Configuring the Hello Time

To configure the hello interval for the spanning tree, use the following command in global configuration mode:

Command	Purpose
`Router(config)# [`**`no`**`]` **`spanning-tree vlan`** *`vlan_ID`* **`hello-time`** *`hello_time`*	Configures the hello time of a VLAN. The **hello_time** value can be from 1 to 10 seconds. Use the **no** form of this command to restore the defaults.

Configuring the Forward-Delay Time for a VLAN

To configure the forward delay for the spanning tree, use the following command in global configuration mode:

Command	Purpose
Router(config)# [**no**] **spanning-tree vlan** *vlan_ID* **forward-time** *forward_time*	Configures the forward time of a VLAN. The value of **forward_time** can be from 4 to 30 seconds. Use the **no** form of this command to restore the defaults.

Configuring the Maximum Aging Time for a VLAN

To configure the maximum age interval for the spanning tree, use the following command in global configuration mode:

Command	Purpose
Router(config)# [**no**] **spanning-tree vlan** *vlan_ID* **max-age** *max_age*	Configures the maximum aging time of a VLAN. The value of **max_age** can be from 6 to 40 seconds. Use the **no** form of this command to restore the defaults.

Configuring the Root Bridge

The EtherSwitch HWIC maintains a separate instance of spanning tree for each active VLAN configured on the switch. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the switch with the lowest bridge ID will become the root bridge for that VLAN.

To configure a VLAN instance to become the root bridge, the bridge priority can be modified from the default value (32768) to a significantly lower value so that the bridge becomes the root bridge for the specified VLAN. Use the spanning-tree vlan vlan-ID root command to alter the bridge priority.

The switch checks the bridge priority of the current root bridges for each VLAN. The bridge priority for the specified VLANs is set to 8192 if this value will cause the switch to become the root for the specified VLANs.

If any root switch for the specified VLANs has a bridge priority lower than 8192, the switch sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

For example, if all switches in the network have the bridge priority for VLAN 100 set to the default value of 32768, entering the spanning-tree vlan 100 root primary command on a switch will set the bridge priority for VLAN 100 to 8192, causing the switch to become the root bridge for VLAN 100.

Note Note The root switch for each instance of spanning tree should be a backbone or distribution switch. Do not configure an access switch as the spanning tree primary root.

Use the diameter keyword to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two end stations in the Layer 2 network). When you specify the network diameter, the switch automatically picks an optimal hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the spanning tree convergence time. You can use the hello keyword to override the automatically calculated hello time.

Note Note We recommend that you avoid configuring the hello time, forward delay time, and maximum age time manually after configuring the switch as the root bridge.

To configure the switch as the root, use the following command in global configuration mode:

Command	Purpose
`Router(config)# [no] spanning-tree vlan vlan_ID root primary [diameter hops [hello-time seconds]]`	Configures a switch as the root switch. Use the **no** form of this command to restore the defaults.

Disabling Spanning Tree

To disable spanning tree on a per-VLAN basis, use the following command in global configuration mode:

Command	Purpose
`Router(config)# no spanning-tree vlan vlan_ID`	Disables spanning tree on a per-VLAN basis.

Verifying that Spanning Tree is Disabled.

Use the **show spanning-tree vlan** to verify the that the spanning tree is disabled, as illustrated below:

```
Router# show spanning-tree vlan 200
<output truncated>
Spanning tree instance for VLAN 200 does not exist.
Router#
```

Configuring MAC Table Manipulation

Port security is implemented by providing the user with the option to make a port secure by allowing only well-known MAC addresses to send in data traffic. Up to 200 secure MAC addresses per HWIC are supported.

- Enabling Known MAC Address Traffic, page 32
- Creating a Static Entry in the MAC Address Table, page 33
- Configuring the Aging Timer, page 34
- Verifying the Aging Time, page 34

Enabling Known MAC Address Traffic

Beginning in privileged EXEC mode, follow these steps to enable the MAC address secure option.

SUMMARY STEPS

1. `configure terminal`
2. `[no] mac-address-table secure <mac-address> fastethernet interface-id [vlan <vlan id>]`
3. `end`

DETAILED STEPS

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# [no] mac-address-table secure <mac-address> fastethernet interface-id [vlan <vlan id>]`	Secures the MAC address traffic on the port.
Step 3	`Router(config)# end`	Exits configuration mode.

Verifying the MAC Address Table Secure Option

Use the **show mac-address-table secure** to verify the configuration, as illustrated below:

```
Router# show mac-address-table secure

Secure Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0000.0002.0001          Secure        2     FastEthernet0/1/1
```

Creating a Static Entry in the MAC Address Table

Beginning in privileged EXEC mode, follow these steps to create a static entry in the MAC address table.

SUMMARY STEPS

1. **configure terminal**
2. **mac-address-table static** *mac-address* **fastethernet** *interface-id* [**vlan** <*vlan id*>]
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router# configure terminal`	Enters global configuration mode.
Step 2	`Router(config)# mac-address-table static mac-address fastethernet interface-id [vlan <vlan id>]`	Creates static entry in the MAC address table. When vlan-id is not specified, VLAN 1 is taken by default.
Step 3	`Router(config)# end`	Exits configuration mode.

Verifying the Mac Address Table

Use the **show mac** command to verify the MAC address table, as illustrated below:

```
Router# show mac-address-table

Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
00ff.ff0d.2dc0          Self          1    Vlan1
0007.ebc7.ff84          Static        1    FastEthernet0/3/5
```

```
0007.ebc8.018b         Static       1    FastEthernet0/3/6
000b.bf94.0006         Static       1    FastEthernet0/3/3
000b.bf94.0038         Static       1    FastEthernet0/3/0
000b.bf94.0039         Static       1    FastEthernet0/3/1
000b.bf94.0008         Static     314    FastEthernet0/3/2
000b.bf94.0038         Static     314    FastEthernet0/3/0
000b.bf94.0008         Static     331    FastEthernet0/3/2
000b.bf94.0038         Static     331    FastEthernet0/3/0
000b.bf94.0008         Static     348    FastEthernet0/3/2
000b.bf94.0038         Static     348    FastEthernet0/3/0
```

Configuring the Aging Timer

The aging timer may be configured from 16 seconds to 4080 seconds, in 16-second intervals.

Beginning in privileged EXEC mode, follow these steps to configure the aging timer.

SUMMARY STEPS

1. **configure terminal**
2. **mac-address-table aging-time** <10-1000000>
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **mac-address-table aging-time** <10-1000000>	Configures the MAC address aging timer age in seconds
Step 3	Router(config)# **end**	Exits configuration mode.

Caution Cisco advises that you not change the aging timer, because the EtherSwitch HWIC could go out of synchronization.

Verifying the Aging Time

Use the **show mac-address-table aging-time** command to verify the MAC address table aging timer, as illustrated below:

```
Router # show mac-address-table aging-time
Mac address aging time 320
```

Configuring Cisco Discovery Protocol

- Enabling Cisco Discovery Protocol, page 35
- Enabling CDP on an Interface, page 35
- Monitoring and Maintaining CDP, page 36

Enabling Cisco Discovery Protocol

To enable Cisco Discovery Protocol (CDP) globally, use the following command in global configuration mode:

Command	Purpose
`Router(config)# cdp run`	Enables CDP globally.

Verifying the CDP Global Configuration

Use the **show cdp** command to verify the CDP configuration:

```
Router# show cdp

Global CDP information:
        Sending CDP packets every 120 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
Router#
```

Enabling CDP on an Interface

To enable CDP on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# cdp enable`	Enables CDP on an interface.

The following example shows how to enable CDP on Fast Ethernet interface 0/1/1:

```
Router(config)# interface fastethernet 0/1/1
Router(config-if)# cdp enable
```

Verifying the CDP Interface Configuration

Use the **show cdp interface** command to verify the CDP configuration for an interface:

```
Router# show cdp interface fastethernet 0/1/1

FastEthernet0/1/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 120 seconds
  Holdtime is 180 seconds
Router#
```

Verifying CDP Neighbors

Use the **show cdp neighbors** command to verify information about the neighboring equipment:

```
Router# show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
tftp-switch      Fas 0/0              125       R S I     2811      Fas 0/3/6
hwic-3745-2      Fas 0/1/0            149       R S I     3745      Fas 0/1
Router#
```

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, use one or more of the following commands in privileged EXEC mode:

Command	Purpose
`Router# clear cdp counters`	Resets the traffic counters to zero.
`Router# clear cdp table`	Deletes the CDP table of information about neighbors.
`Router# show cdp`	Verifies global information such as frequency of transmissions and the holdtime for packets being transmitted.
`Router# show cdp entry entry_name [protocol | version]`	Verifies information about a specific neighbor. The display can be limited to protocol version information.
`Router# show cdp interface interface-id`	Verifies information about interfaces on which CDP is enabled.
`Router# show cdp neighbors interface-id [detail]`	Verifies information about neighbors. The display can be limited to neighbors on a specific interface and can be expanded to provide more detailed information.
`Router# show cdp traffic`	Verifies CDP counters, including the number of packets sent and received and checksum errors.

Configuring the Switched Port Analyzer (SPAN)

This section describes how to configure a SPAN session for an EtherSwitch HWIC.

Note An EtherSwitch HWIC supports only one SPAN session.

Note Either Tx or both Tx and Rx monitoring is supported.

- Configuring the SPAN Sources, page 36
- Configuring SPAN Destinations, page 37
- Verifying the SPAN Session, page 37
- Removing Sources or Destinations from a SPAN Session, page 37

Configuring the SPAN Sources

To configure the source for a SPAN session, use the following command in global configuration mode:

Command	Purpose
`Router(config)# monitor session 1 {source {interface interface-id} | {vlan vlan_ID}} [, | - | rx | tx | both]`	Specifies the SPAN session (number 1), the source interfaces or VLANs, and the traffic direction to be monitored.

The following example shows how to configure the SPAN session to monitor bidirectional traffic from source interface Fast Ethernet 0/3/1:

```
Router(config)# monitor session 1 source interface fastethernet 0/3/1
```

Configuring SPAN Destinations

To configure the destination for a SPAN session, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`monitor session 1 {destination {interface`** *`type interface-id`*`} [, | -] | {`**`vlan`** *`vlan`*`_ID}}`	Specifies the SPAN session (number 1) and the destination interfaces or VLANs.

Verifying the SPAN Session

Use the **show monitor session** command to verify the sources and destinations configured for the SPAN session.

```
Router# show monitor session 1
Session 1
---------
Source Ports:
 RX Only: None
 TX Only: None
 Both: Fa0/1/0
Source VLANs:
 RX Only: None
 TX Only: None
 Both: None
Destination Ports: Fa0/1/1
Filter VLANs: None
```

Removing Sources or Destinations from a SPAN Session

To remove sources or destinations from the SPAN session, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`no monitor session 1`**	Clears existing SPAN configuration.

Configuring Power Management on the Interface

Beginning in privileged EXEC mode, follow these steps to manage the powering of the Cisco IP phones.

SUMMARY STEPS

1. **`configure terminal`**
2. **`interface fastethernet`** *`interface-id`*
3. **`power inline auto/never`**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`interface fastethernet`** *`interface-id`*	Selects a particular Fast Ethernet interface for configuration.
Step 3	`Router(config-if)#` **`power inline auto`**`/`**`never`**	Configures the port to supply inline power automatically to a Cisco IP phone. Use **never** to permanently disable inline power on the port.

Verifying Power Management on the Interface

Use the **show power inline** command to verify the power configuration on the ports, as illustrated below:

```
Router# show power inline

PowerSupply   SlotNum.   Maximum   Allocated    Status
-----------   --------   -------   ---------    ------
 INT-PS          0       120.000    101.500     PS GOOD

Interface     Config     Phone     Powered      PowerAllocated
---------     ------     -----     -------      --------------
Fa0/1/0         auto       Cisco     On           6.300 Watts
Fa0/1/1         auto       Cisco     On           6.300 Watts
Fa0/1/2         auto       Cisco     On           6.300 Watts
Fa0/1/3         auto       Cisco     On           6.300 Watts
Fa0/1/4         auto       Cisco     On           6.300 Watts
Fa0/1/5         auto       Cisco     On           6.300 Watts
Fa0/1/6         auto       Cisco     On           6.300 Watts
Fa0/1/7         auto       Cisco     On           6.300 Watts
Fa0/3/0         auto       Cisco     On           6.300 Watts
Fa0/3/1         auto       Cisco     On           6.300 Watts
Fa0/3/2         auto       Cisco     On           6.300 Watts
Fa0/3/3         auto       Cisco     On           6.300 Watts
Fa0/3/4         auto       Cisco     On           6.300 Watts
Fa0/3/5         auto       Cisco     On           6.300 Watts
Fa0/3/6         auto       IEEE-2    On           7.000 Watts
Fa0/3/7         auto       Cisco     On           6.300 Watts
```

Verifying Other Power Management CLI

Use the **show power inline** command to verify the power configuration on the ports, as illustrated below:

```
Router# show power inline [actual | interface fastethernet interface-id | configured]
```

Configuring IP Multicast Layer 3 Switching

These sections describe how to configure IP multicast Layer 3 switching:

- Enabling IP Multicast Routing Globally, page 39
- Enabling IP Protocol-Independent Multicast (PIM) on Layer 3 Interfaces, page 39
- Verifying IP Multicast Layer 3 Hardware Switching Summary, page 40
- Verifying the IP Multicast Routing Table, page 41

Enabling IP Multicast Routing Globally

You must enable IP multicast routing globally before you can enable IP multicast Layer 3 switching on Layer 3 interfaces.

For complete information and procedures, refer to these publications:

- *Cisco IOS IP Configuration Guide*, Release 12.2, at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*, Release 12.2 at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*, Release 12.2 at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/index.htm
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*, Release 12.2 at this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprmc_r/index.htm

To enable IP multicast routing globally, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip multicast-routing`	Enables IP multicast routing globally.

Enabling IP Protocol-Independent Multicast (PIM) on Layer 3 Interfaces

You must enable PIM on the Layer 3 interfaces before enabling IP multicast Layer 3 switching functions on those interfaces.

Beginning in global configuration mode, follow these steps to enable IP PIM on a Layer 3 interface.

SUMMARY STEPS

1. **interface vlan** *vlan-id*
2. **ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**}

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#` **`interface vlan`** *`vlan-id`*	Selects the interface to be configured.
Step 2	`Router(config-if)#` **`ip pim {dense-mode	sparse-mode	sparse-dense-mode}`**	Enables IP PIM on a Layer 3 interface.

The following example shows how to enable PIM on an interface using the default mode (**sparse-dense-mode**):

```
Router(config-if)# ip pim sparse-dense mode
Router(config-if)#
```

The following example shows how to enable PIM sparse mode on an interface:

```
Router(config-if)# ip pim sparse-mode
Router(config-if)#
```

Verifying IP Multicast Layer 3 Hardware Switching Summary

Note The **show interface statistics** command does not verify hardware-switched packets, only packets switched by software.

The **show ip pim interface count** command verifies the IP multicast Layer 3 switching enable state on IP PIM interfaces and the number of packets received and sent on the interface.

Use the following **show** commands to verify IP multicast Layer 3 switching information for an IP PIM Layer 3 interface.

Step 1

```
Router# show ip pim interface count

State:* - Fast Switched, D - Distributed Fast Switched
      H - Hardware Switching Enabled
Address          Interface           FS  Mpackets In/Out
10.0.0.1         VLAN1               *   151/0
Router#
```

Step 2

```
Router# show ip mroute count

IP Multicast Statistics
5 routes using 2728 bytes of memory
4 groups, 0.25 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:224.9.9.9, Source count:1, Packets forwarded: 0, Packets received: 66
  Source:10.0.0.2/32, Forwarding:0/0/0/0, Other:66/0/66
Group:224.10.10.10, Source count:0, Packets forwarded: 0, Packets received: 0
Group:224.0.1.39, Source count:0, Packets forwarded: 0, Packets received: 0
Group:224.0.1.40, Source count:0, Packets forwarded: 0, Packets received: 0
Router#
```

Note A negative counter means that the outgoing interface list of the corresponding entry is NULL, and this indicates that this flow is still active.

Step 3

```
Router# show ip interface vlan 1

Vlan1 is up, line protocol is up
  Internet address is 10.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.2 224.0.0.22 224.0.0.13
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
Router#
```

Verifying the IP Multicast Routing Table

Use the **show ip mroute** command to verify the IP multicast routing table:

```
Router# show ip mroute 224.10.103.10

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched, A - Assert winner
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode
```

```
(*, 224.10.10.10), 00:09:21/00:02:56, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse-Dense, 00:09:21/00:00:00, H

Router#
```

Note The RPF-MFD flag indicates that the flow is completely hardware switched. The H flag indicates that the flow is hardware-switched on the outgoing interface.

Configuring IGMP Snooping

This section describes how to configure IGMP snooping on your router and consists of the following configuration information and procedures:

- Enabling or Disabling IGMP Snooping, page 42
- Enabling IGMP Immediate-Leave Processing, page 43
- Statically Configuring an Interface to Join a Group, page 44
- Configuring a Multicast Router Port, page 45

Enabling or Disabling IGMP Snooping

By default, IGMP snooping is globally enabled on the EtherSwitch HWIC. When globally enabled or disabled, it is also enabled or disabled in all existing VLAN interfaces. By default, IGMP snooping is enabled on all VLANs, but it can be enabled and disabled on a per-VLAN basis.

Global IGMP snooping overrides the per-VLAN IGMP snooping capability. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you can enable or disable snooping on a VLAN basis.

Beginning in privileged EXEC mode, follow these steps to globally enable IGMP snooping on the EtherSwitch HWIC.

SUMMARY STEPS

1. **`configure terminal`**
2. **`ip igmp snooping`**
3. **`end`**
4. **`show ip igmp snooping`**
5. **`copy running-config startup-config`**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`ip igmp snooping`**	Globally enables IGMP snooping in all existing VLAN interfaces.
Step 3	**`end`**	Returns to privileged EXEC mode.

	Command	Purpose
Step 4	`show ip igmp snooping`	Displays snooping configuration.
Step 5	`copy running-config startup-config`	(Optional) Saves your configuration to the startup configuration.

To globally disable IGMP snooping on all VLAN interfaces, use the **no ip igmp snooping** global command.

Beginning in privileged EXEC mode, follow these steps to enable IGMP snooping on a VLAN interface.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping vlan** *vlan-id*
3. **end**
4. **show ip igmp snooping** [**vlan** *vlan-id*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.
Step 2	`ip igmp snooping vlan` *vlan-id*	Enables IGMP snooping on the VLAN interface.
Step 3	`end`	Returns to privileged EXEC mode.
Step 4	`show ip igmp snooping [vlan` *vlan-id*`]`	Displays snooping configuration. (Optional) *vlan-id* is the number of the VLAN.
Step 5	`copy running-config startup-config`	(Optional) Saves your configuration to the startup configuration.

To disable IGMP snooping on a VLAN interface, use the **no ip igmp snooping vlan** *vlan-id* global configuration command for the specified VLAN number (for example, vlan1).

Enabling IGMP Immediate-Leave Processing

When you enable IGMP Immediate-Leave processing, the EtherSwitch HWIC immediately removes a port from the IP multicast group when it detects an IGMP version 2 leave message on that port. Immediate-Leave processing allows the switch to remove an interface that sends a leave message from the forwarding table without first sending out group-specific queries to the interface. You should use the Immediate-Leave feature only when there is only a single receiver present on every port in the VLAN.

Beginning in privileged EXEC mode, follow these steps to enable IGMP Immediate-Leave processing.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping vlan** *vlan-id* **immediate-leave**
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip igmp snooping vlan** *vlan-id* **immediate-leave**	Enables IGMP Immediate-Leave processing on the VLAN interface.
Step 3	**end**	Returns to privileged EXEC mode.

To disable Immediate-Leave processing, follow Steps 1 and 2 to enter interface configuration mode, and use the **no ip igmp snooping vlan** *vlan-id* **immediate-leave** global configuration command.

Statically Configuring an Interface to Join a Group

Ports normally join multicast groups through the IGMP report message, but you can also statically configure a host on an interface.

Beginning in privileged EXEC mode, follow these steps to add a port as a member of a multicast group.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id*
3. **end**
4. **show mac-address-table multicast** [**vlan** *vlan-id*] [**user** | **igmp-snooping**] [**count**]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode
Step 2	**ip igmp snooping vlan** *vlan-id* **static** *mac-address* **interface** *interface-id*	Statically configures a port as a member of a multicast group: • *vlan-id* is the multicast group VLAN ID. • *mac-address* is the group MAC address. • *interface-id* is the member port.
Step 3	**end**	Returns to privileged EXEC mode.

	Command	Purpose
Step 4	**show mac-address-table multicast** [**vlan** *vlan-id*] [**user** | **igmp-snooping**] [**count**]	Displays MAC address table entries for a VLAN. • *vlan-id* is the multicast group VLAN ID. • **user** displays only the user-configured multicast entries. • **igmp-snooping** displays entries learned via IGMP snooping. • **count** displays only the total number of entries for the selected criteria, not the actual entries.
Step 5	**copy running-config startup-config**	(Optional) Saves your configuration to the startup configuration.

Configuring a Multicast Router Port

Beginning in privileged EXEC mode, follow these steps to enable a static connection to a multicast router.

SUMMARY STEPS

1. **configure terminal**
2. **ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}
3. **end**
4. **show ip igmp snooping** [**vlan** *vlan-id*]
5. **show ip igmp snooping mrouter** [**vlan** *vlan-id*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}	Specify the multicast router VLAN ID (1 to 1001). Specify the interface to the multicast router.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show ip igmp snooping** [**vlan** *vlan-id*]	Verifies that IGMP snooping is enabled on the VLAN interface.
Step 5	**show ip igmp snooping mrouter** [**vlan** *vlan-id*]	Displays information on dynamically learned and manually configured multicast router interfaces.
Step 6	**copy running-config startup-config**	(Optional) Saves your configuration to the startup configuration.

Configuring Per-Port Storm-Control

You can use these techniques to block the forwarding of unnecessary flooded traffic. This section describes how to configure per-port storm-control and characteristics on your router and consists of the following configuration procedures:

- Enabling Per-Port Storm-Control, page 46
- Disabling Per-Port Storm-Control, page 47

By default, unicast, broadcast, and multicast suppression is disabled.

Enabling Per-Port Storm-Control

Beginning in privileged EXEC mode, follow these steps to enable per-port storm-control.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** *level-high* [*level-low*]
4. **storm-control action shutdown**
5. **end**
6. **show storm-control** [**interface**] [{**broadcast** | **multicast** | **unicast** | **history**}]

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Enters interface configuration mode, and enter the port to configure.
Step 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level** *level-high* [*level-low*]	Configures broadcast, multicast, or unicast per-port storm-control. Specify the rising threshold level for either broadcast, multicast, or unicast traffic. The storm control action occurs when traffic utilization reaches this level. (Optional) Specify the falling threshold level. The normal transmission restarts (if the action is filtering) when traffic drops below this level.
Step 4	**storm-control action shutdown**	Selects the **shutdown** keyword to disable the port during a storm. The default is to filter out the traffic.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show storm-control** [**interface**] [{**broadcast** | **multicast** | **unicast** | **history**}]	Verifies your entries.

Note If any type of traffic exceeds the upper threshold limit, all of the other types of traffic will be stopped.

Disabling Per-Port Storm-Control

Beginning in privileged EXEC mode, follow these steps to disable per-port storm-control.

SUMMARY STEPS

1. **`configure terminal`**
2. **`interface`** *`interface-id`*
3. **`no storm-control {broadcast | multicast | unicast} level`**
4. **`no storm-control action shutdown`**
5. **`end`**
6. **`show storm-control {broadcast | multicast | unicast}`**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`interface`** *`interface-id`*	Enters interface configuration mode, and enter the port to configure.
Step 3	**`no storm-control {broadcast	multicast	unicast} level`**	Disables per-port storm control.
Step 4	**`no storm-control action shutdown`**	Disables the specified storm control action.
Step 5	**`end`**	Returns to privileged EXEC mode.
Step 6	**`show storm-control {broadcast	multicast	unicast}`**	Verifies your entries.

Configuring Stacking

Stacking is the connection of two switch modules resident in the same chassis so that they behave as a single switch. When a chassis is populated with two switch modules, the user must configure both of them to operate in stacked mode. This is done by selecting one port from each switch module and configuring it to be a stacking partner. The user must then connect with a cable the stacking partners from each switch module to physically stack the switch modules. Any one port in a switch module can be designated as the stacking partner for that switch module.

Beginning in privileged EXEC mode, follow these steps to configure a pair of ports on two different switch modules as stacking partners.

SUMMARY STEPS

1. **`interface fastethernet`** *`interface-id`*
2. **`no shutdown`**
3. **`switchport stacking-partner interface FastEthernet`** *`partner-interface-id`*

4. **exit**
5. **interface fastethernet** partner-*interface-id*
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#`**`interface fastethernet`** *`interface-id`*	Selects the interface to configure.
Step 2	`Router(config-if)#`**`no shutdown`**	Activates the interface. (Required only if you shut down the interface.)
Step 3	`Router(config-if)#`**`switchport stacking-partner interface FastEthernet`** *`partner-interface-id`*	Selects and configures the stacking partner port. To restore the defaults, use the **no** form of this command.
Step 4	`Router(config-if)#`**`exit`**	Exits interface configuration mode.
Step 5	`Router(config)#`**`interface fastethernet`** `partner-`*`interface-id`*	Selects the stacking partner interface.
Step 6	`Router(config-if)#`**`no shutdown`**	Activates the stacking partner interface.
Step 7	`Router(config-if)#`**`end`**	Exits configuration mode.

Note Both stacking partner ports must have their **speed** and **duplex** parameters set to **auto**.

Caution If stacking is removed, stacked interfaces will go to **shutdown** state. Other non-stacked ports will be left unchanged.

Configuring Fallback Bridging

This section describes how to configure fallback bridging on your switch. It contains this configuration information:

- Understanding the Default Fallback Bridging Configuration, page 49
- Creating a Bridge Group, page 49
- Preventing the Forwarding of Dynamically Learned Stations, page 51
- Configuring the Bridge Table Aging Time, page 51
- Filtering Frames by a Specific MAC Address, page 52
- Adjusting Spanning-Tree Parameters, page 53
- Monitoring and Maintaining the Network, page 59

Understanding the Default Fallback Bridging Configuration

Table 2 shows the default fallback bridging configuration.

Table 2 Default Fallback Bridging Configuration

Feature	Default Setting
Bridge groups	None are defined or assigned to an interface. No VLAN-bridge STP is defined.
Switch forwards frames for stations that it has dynamically learned	Enabled.
Bridge table aging time for dynamic entries	300 seconds.
MAC-layer frame filtering	Disabled.
Spanning tree parameters: • Switch priority • Interface priority • Interface path cost • Hello BPDU interval • Forward-delay interval • Maximum idle interval	 • 32768. • 128. • 10 Mbps: 100. 100 Mbps: 19. 1000 Mbps: 4. • 2 seconds. • 20 seconds. • 30 seconds.

Creating a Bridge Group

To configure fallback bridging for a set of SVIs, these interfaces must be assigned to bridge groups. All interfaces in the same group belong to the same bridge domain. Each SVI can be assigned to only one bridge group.

Beginning in privileged EXEC mode, follow these steps to create a bridge group and assign an interface to it.

SUMMARY STEPS

1. **configure terminal**
2. **no ip routing**
3. **bridge** *bridge-group* **protocol vlan-bridge**
4. **interface** *interface-id*
5. **bridge-group** *bridge-group*
6. **end**
7. **show vlan-bridge**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`no ip routing`**	Disables ip routing.
Step 3	**`bridge`** *`bridge-group`* **`protocol vlan-bridge`**	Assigns a bridge group number, and specify the VLAN-bridge spanning-tree protocol to run in the bridge group. The **ibm** and **dec** keywords are not supported. For *bridge-group*, specify the bridge group number. The range is 1 to 255. Frames are bridged only among interfaces in the same group.
Step 4	**`interface`** *`interface-id`*	Enters interface configuration mode and specifies the interface on which you want to assign the bridge group. The specified interface must be an SVI: a VLAN interface that you created by using the **interface vlan** *vlan-id* global configuration command. These ports must have IP addresses assigned to them.
Step 5	**`bridge-group`** *`bridge-group`*	Assigns the interface to the bridge group created in Step 2. By default, the interface is not assigned to any bridge group. An interface can be assigned to only one bridge group.
Step 6	**`end`**	Returns to privileged EXEC mode.
Step 7	**`show vlan-bridge`**	(Optional) Verifies forwarding mode.
Step 8	**`show running-config`**	(Optional) Verifies your entries.
Step 9	**`copy running-config startup-config`**	(Optional) Saves your entries in the configuration file.

To remove a bridge group, use the **no bridge** *bridge-group* **protocol vlan-bridge** global configuration command. To remove an interface from a bridge group, use the **no bridge-group** *bridge-group* interface configuration command.

Preventing the Forwarding of Dynamically Learned Stations

By default, the switch forwards any frames for stations that it has dynamically learned. By disabling this activity, the switch only forwards frames whose addresses have been statically configured into the forwarding cache.

Beginning in privileged EXEC mode, follow these steps to prevent the switch from forwarding frames for stations that it has dynamically learned.

SUMMARY STEPS

1. **configure terminal**
2. **no bridge** *bridge-group* **acquire**
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**no bridge** *bridge-group* **acquire**	Enables the switch to stop forwarding any frames for stations that it has dynamically learned through the discovery process and to limit frame forwarding to statically configured stations. The switch filters all frames except those whose destined-to addresses have been statically configured into the forwarding cache. To configure a static address, use the **bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} global configuration command. For *bridge-group*, specify the bridge group number. The range is 1 to 255.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entry.
Step 5	**copy running-config startup-config**	(Optional) Saves your entry in the configuration file.

To cause the switch to forward frames to stations that it has dynamically learned, use the **bridge** *bridge-group* **acquire** global configuration command.

Configuring the Bridge Table Aging Time

A switch forwards, floods, or drops packets based on the bridge table. The bridge table maintains both static and dynamic entries. Static entries are entered by you. Dynamic entries are entered by the bridge learning process. A dynamic entry is automatically removed after a specified length of time, known as aging time, from the time the entry was created or last updated.

If you are likely to move hosts on a switched network, decrease the aging-time to enable the switch to quickly adapt to the change. If hosts on a switched network do not continuously send packets, increase the aging time to keep the dynamic entries for a longer time and thus reduce the possibility of flooding when the hosts send again.

Beginning in privileged EXEC mode, follow these steps to configure the aging time.

SUMMARY STEPS

1. **configure terminal**
2. **bridge** *bridge-group* **aging-time** *seconds*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**bridge** *bridge-group* **aging-time** *seconds*	Specifies the length of time that a dynamic entry remains in the bridge table from the time the entry was created or last updated. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 0 to 1000000. The default is 300 seconds.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entry.
Step 5	**copy running-config startup-config**	(Optional) Saves your entry in the configuration file.

To return to the default aging-time interval, use the **no bridge** *bridge-group* **aging-time** global configuration command.

Filtering Frames by a Specific MAC Address

A switch examines frames and sends them through the internetwork according to the destination address; a switch does not forward a frame back to its originating network segment. You can use the software to configure specific administrative filters that filter frames based on information other than the paths to their destinations.

You can filter frames with a particular MAC-layer station destination address. Any number of addresses can be configured in the system without a performance penalty.

Beginning in privileged EXEC mode, follow these steps to filter by the MAC-layer address.

SUMMARY STEPS

1. **configure terminal**
2. **bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-id*]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**bridge** *bridge-group* **address** *mac-address* {**forward** | **discard**} [*interface-id*]	Specifies the MAC address to discard or forward. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For **address** *mac-address*, specify the MAC-layer destination address to be filtered. • Specify **forward** if you want the frame destined to the specified interface to be forwarded. Specify **discard** if you want the frame to be discarded. • (Optional) For *interface-id*, specify the interface on which the address can be reached.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entry.
Step 5	**copy running-config startup-config**	(Optional) Saves your entry in the configuration file.

To disable the frame forwarding ability, use the **no bridge** *bridge-group* **address** *mac-address* global configuration command.

Adjusting Spanning-Tree Parameters

You might need to adjust certain spanning-tree parameters if the default values are not suitable for your switch configuration. Parameters affecting the entire spanning tree are configured with variations of the **bridge** global configuration command. Interface-specific parameters are configured with variations of the **bridge-group** interface configuration command.

You can adjust spanning-tree parameters by performing any of the tasks in these sections:

- Changing the Switch Priority, page 54
- Changing the Interface Priority, page 54
- Assigning a Path Cost, page 55
- Adjusting BPDU Intervals, page 56
- Disabling the Spanning Tree on an Interface, page 58

Note Only network administrators with a good understanding of how switches and STP function should make adjustments to spanning-tree parameters. Poorly planned adjustments can have a negative impact on performance. A good source on switching is the IEEE 802.1d specification; for more information, refer to the “References and Recommended Reading” appendix in the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2.

Changing the Switch Priority

You can globally configure the priority of an individual switch when two switches tie for position as the root switch, or you can configure the likelihood that a switch will be selected as the root switch. This priority is determined by default; however, you can change it.

Beginning in privileged EXEC mode, follow these steps to change the switch priority.

SUMMARY STEPS

1. **`configure terminal`**
2. **`bridge`** *`bridge-group`* **`priority`** *`number`*
3. **`end`**
4. **`show running-config`**
5. **`copy running-config startup-config`**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`bridge`** *`bridge-group`* **`priority`** *`number`*	Changes the priority of the switch. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *number*, enter a number from 0 to 65535. The default is 32768. The lower the number, the more likely the switch will be chosen as the root.
Step 3	**`end`**	Returns to privileged EXEC mode.
Step 4	**`show running-config`**	Verifies your entry.
Step 5	**`copy running-config startup-config`**	(Optional) Saves your entry in the configuration file.

No **no** form of this command exists. To return to the default setting, use the **bridge** *bridge-group* **priority** *number* global configuration command, and set the priority to the default value. To change the priority on an interface, use the **bridge-group priority** interface configuration command (described in the next section).

Changing the Interface Priority

You can change the priority for an interface. When two switches tie for position as the root switch, you configure an interface priority to break the tie. The switch with the lowest interface value is elected.

Beginning in privileged EXEC mode, follow these steps to change the interface priority.

SUMMARY STEPS

1. **`configure terminal`**
2. **`interface`** *`interface-id`*
3. **`bridge-group`** *`bridge-group`* **`priority`** *`number`*

4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Enters interface configuration mode, and specifies the interface to set the priority.
Step 3	**bridge-group** *bridge-group* **priority** *number*	Changes the priority of an interface. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *number*, enter a number from 0 to 255. The lower the number, the more likely that the interface on the switch will be chosen as the root. The default is 128.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show running-config**	Verifies your entry.
Step 6	**copy running-config startup-config**	(Optional) Saves your entry in the configuration file.

To return to the default setting, use the **bridge-group** *bridge-group* **priority** *number* interface configuration command.

Assigning a Path Cost

Each interface has a path cost associated with it. By convention, the path cost is 1000/data rate of the attached LAN, in Mbps.

Beginning in privileged EXEC mode, follow these steps to assign a path cost.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **bridge-group** *bridge-group* **path-cost** *cost*
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	`configure terminal`	Enters global configuration mode.
Step 2	**interface** *interface-id*	Enters interface configuration mode, and specify the interface to set the path cost.
Step 3	**bridge-group** *bridge-group* **path-cost** *cost*	Assigns the path cost of an interface. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *cost*, enter a number from 1 to 65536. The higher the value, the higher the cost. – For 10 Mbps, the default path cost is 100. – For 100 Mbps, the default path cost is 19. – For 1000 Mbps, the default path cost is 4.
Step 4	`end`	Returns to privileged EXEC mode.
Step 5	`show running-config`	Verifies your entry.
Step 6	`copy running-config startup-config`	(Optional) Saves your entry in the configuration file.

To return to the default path cost, use the **no bridge-group** *bridge-group* **path-cost** *cost* interface configuration command.

Adjusting BPDU Intervals

You can adjust BPDU intervals as described in these sections:

- Adjusting the Interval between Hello BPDUs, page 56
- Changing the Forward-Delay Interval, page 57
- Changing the Maximum-Idle Interval, page 58

Note Each switch in a spanning tree adopts the interval between hello BPDUs, the forward delay interval, and the maximum idle interval parameters of the root switch, regardless of what its individual configuration might be.

Adjusting the Interval between Hello BPDUs

Beginning in privileged EXEC mode, follow these step to adjust the interval between hello BPDUs.

SUMMARY STEPS

1. `configure terminal`
2. **bridge** *bridge-group* **hello-time** *seconds*
3. `end`
4. `show running-config`
5. `copy running-config startup-config`

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**bridge** *bridge-group* **hello-time** *seconds*	Specifies the interval between hello BPDUs. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 1 to 10. The default is 2 seconds.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entry.
Step 5	**copy running-config startup-config**	(Optional) Saves your entry in the configuration file.

To return to the default setting, use the **no bridge** *bridge-group* **hello-time** global configuration command.

Changing the Forward-Delay Interval

The forward-delay interval is the amount of time spent listening for topology change information after an interface has been activated for switching and before forwarding actually begins.

Beginning in privileged EXEC mode, follow these steps to change the forward-delay interval.

SUMMARY STEPS

1. **configure terminal**
2. **bridge** *bridge-group* **forward-time** *seconds*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**bridge** *bridge-group* **forward-time** *seconds*	Specifies the forward-delay interval. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 10 to 200. The default is 20 seconds.
Step 3	**end**	Returns to privileged EXEC mode.
Step 4	**show running-config**	Verifies your entry.
Step 5	**copy running-config startup-config**	(Optional) Saves your entry in the configuration file.

To return to the default setting, use the **no bridge** *bridge-group* **forward-time** *seconds* global configuration command.

Changing the Maximum-Idle Interval

If a switch does not hear BPDUs from the root switch within a specified interval, it recomputes the spanning-tree topology.

Beginning in privileged EXEC mode, follow these steps to change the maximum-idle interval (maximum aging time).

SUMMARY STEPS

1. **`configure terminal`**
2. **`bridge`** *`bridge-group`* **`max-age`** *`seconds`*
3. **`end`**
4. **`show running-config`**
5. **`copy running-config startup-config`**

DETAILED STEPS

	Command	Purpose
Step 1	**`configure terminal`**	Enters global configuration mode.
Step 2	**`bridge`** *`bridge-group`* **`max-age`** *`seconds`*	Specifies the interval the switch waits to hear BPDUs from the root switch. • For *bridge-group*, specify the bridge group number. The range is 1 to 255. • For *seconds*, enter a number from 10 to 200. The default is 30 seconds.
Step 3	**`end`**	Returns to privileged EXEC mode.
Step 4	**`show running-config`**	Verifies your entry.
Step 5	**`copy running-config startup-config`**	(Optional) Saves your entry in the configuration file.

To return to the default setting, use the **no bridge** *bridge-group* **max-age** global configuration command.

Disabling the Spanning Tree on an Interface

When a loop-free path exists between any two switched subnetworks, you can prevent BPDUs generated in one switching subnetwork from impacting devices in the other switching subnetwork, yet still permit switching throughout the network as a whole. For example, when switched LAN subnetworks are separated by a WAN, BPDUs can be prevented from traveling across the WAN link.

Beginning in privileged EXEC mode, follow these steps to disable spanning tree on an interface.

SUMMARY STEPS

1. **`configure terminal`**
2. **`interface`** *`interface-id`*

3. **bridge-group** *bridge-group* **spanning-disabled**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Enters interface configuration mode, and specify the interface ID.
Step 3	**bridge-group** *bridge-group* **spanning-disabled**	Disables spanning tree on the interface. For *bridge-group*, specify the bridge group number. The range is 1 to 255.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show running-config**	Verifies your entry.
Step 6	**copy running-config startup-config**	(Optional) Saves your entry in the configuration file.

To reenable spanning tree on the interface, use the **no bridge-group** *bridge-group* **spanning-disabled** interface configuration command.

Monitoring and Maintaining the Network

To monitor and maintain the network, use one or more of the following privileged EXEC commands.

Command	Purpose
clear bridge *bridge-group*	Removes any learned entries from the forwarding database and clears the transmit and receive counts for any statically configured entries.
show bridge [*bridge-group*]	Displays details about the bridge group.
show bridge [*bridge-group*] [*interface-id*] [*address*] [**group**] [**verbose**]	Displays classes of entries in the bridge forwarding database.

Configuring Separate Voice and Data Subnets

For ease of network administration and increased scalability, network managers can configure the EtherSwitch HWIC to support Cisco IP phones such that the voice and data traffic reside on separate subnets. You should always use separate VLANs when you are able to segment the existing IP address space of your branch office.

User priority bits in the 802.1p portion of the 802.1Q standard header are used to provide prioritization in Ethernet Switches. This is a vital component in designing Cisco AVVID networks.

The EtherSwitch HWIC provides the performance and intelligent services of Cisco IOS software for branch office applications. The EtherSwitch HWIC can identify user applications—such as voice or multicast video—and classify traffic with the appropriate priority levels.

Note Refer to the *Cisco AVVID QoS Design Guide* for more information on how to implement end-to-end QoS as you deploy Cisco AVVID solutions.

Beginning in global configuration mode, follow these steps to automatically configure Cisco IP phones to send voice traffic on the voice VLAN ID (VVID) on a per-port basis (see the "Voice Traffic and VVID" section on page 60).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **switchport voice vlan** *vlan-id*

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)# enable`	Enters the privileged EXEC mode. A preset password may be required to enter this mode.
Step 2	`Router(config)# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# interface interface-id`	Enters the interface configuration mode and the port to be configured (for example, interface fa0/3/1).
Step 4	`Router(config-if)# switchport mode trunk`	Configures the port to trunk mode.
Step 5	`Router(config-if)# switchport voice vlan vlan-id`	Configures the voice port with a VVID that will be used exclusively for voice traffic.

Voice Traffic and VVID

The EtherSwitch HWIC can automatically configure voice VLAN. This capability overcomes the management complexity of overlaying a voice topology onto a data network while maintaining the quality of voice traffic. With the automatically configured voice VLAN feature, network administrators can segment phones into separate logical networks, even though the data and voice infrastructure is physically the same. The voice VLAN feature places the phones into their own VLANs without the need for end-user intervention. A user can plug the phone into the switch, and the switch provides the phone with the necessary VLAN information.

Configuring a Single Subnet for Voice and Data

For network designs with incremental IP telephony deployment, network managers can configure the EtherSwitch HWIC so that the voice and data traffic coexist on the same subnet. This might be necessary when it is impractical either to allocate an additional IP subnet for IP phones or to divide the existing IP address space into an additional subnet at the remote branch, it might be necessary to use a single IP address space for branch offices. (This is one of the simpler ways to deploy IP telephony.)

This configuration approach must address two key considerations:

- Network managers should ensure that existing subnets have enough available IP addresses for the new Cisco IP phones, each of which requires a unique IP address.
- Administering a network with a mix of IP phones and workstations on the same subnet might pose a challenge.

Beginning in privileged EXEC mode, follow these steps to automatically configure Cisco IP phones to send voice and data traffic on the same VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport access vlan** *vlan-id*
4. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`interface`** *`interface-id`*	Enters the interface configuration mode and the port to be configured (e.g., interface fa0/1/1).
Step 3	`Router(config-if)#` **`switchport access vlan`** *`vlan-id`*	Sets the native VLAN for untagged traffic. The value of *vlan-id* represents the ID of the VLAN that is sending and receiving untagged traffic on the port. Valid IDs are from 1 to 1001. Leading zeroes are not accepted.
Step 4	`Router#` **`end`**	Returns to the privileged EXEC mode.

Verifying Switchport Configuration

Use the **show run interface** command to verify the switchport configuration.

```
Router# show run interface interface-id
```

Use the **write memory** command to save the current configuration in flash memory.

```
Router# write memory
```

Managing the EtherSwitch HWIC

This section describes how to perform basic management tasks on the EtherSwitch HWIC with the Cisco IOS CLI. You might find this information useful when you configure the switch for the previous scenarios.

The following topics are included:

- Adding Trap Managers, page 62
- Configuring IP Information, page 62
- Enabling Switch Port Analyzer, page 65

- Managing the ARP Table, page 66
- Managing the MAC Address Tables, page 66
- Removing Dynamic Addresses, page 68
- Adding Secure Addresses, page 68
- Configuring Static Addresses, page 69
- Clearing all MAC Address Tables, page 71

Adding Trap Managers

A trap manager is a management station that receives and processes traps. When you configure a trap manager, community strings for each member switch must be unique. If a member switch has an IP address assigned to it, the management station accesses the switch by using its assigned IP address.

By default, no trap manager is defined, and no traps are issued.

Beginning in privileged EXEC mode, follow these steps to add a trap manager and community string.

SUMMARY STEPS

1. **configure terminal**
2. **snmp-server host 172.2.128.263** *traps1* **snmp vlan-membership**
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`snmp-server host 172.2.128.263`** *`traps1`* **`snmp vlan-membership`**	Enters the trap manager IP address, community string, and the traps to generate.
Step 3	`Router(config)#` **`end`**	Returns to privileged EXEC mode.

Verifying Trap Managers

Use the **show running-config** command to verify that the information was entered correctly by displaying the running configuration:

```
Router# show running-config
```

Configuring IP Information

This section describes how to assign IP information on the EtherSwitch HWIC. The following topics are included:

- Assigning IP Information to the Switch, page 62
- Specifying a Domain Name and Configuring the DNS, page 64

Assigning IP Information to the Switch

You can use a BOOTP server to automatically assign IP information to the switch; however, the BOOTP server must be set up in advance with a database of physical MAC addresses and corresponding IP addresses, subnet masks, and default gateway addresses. In addition, the switch must be able to access the BOOTP server through one of its ports. At startup, a switch without an IP address requests the information from the BOOTP server; the requested information is saved in the switch running the configuration file. To ensure that the IP information is saved when the switch is restarted, save the configuration by entering the **write memory** command in privileged EXEC mode.

You can change the information in these fields. The mask identifies the bits that denote the network number in the IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask. The broadcast address is reserved for sending messages to all hosts. The CPU sends traffic to an unknown IP address through the default gateway.

Beginning in privileged EXEC mode, follow these steps to enter the IP information.

SUMMARY STEPS

1. **configure terminal**
2. **interface vlan 1**
3. **ip address** *ip-address subnet-mask*
4. **exit**
5. **ip default-gateway** *ip-address*
6. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **configure terminal**	Enters global configuration mode.
Step 2	`Router(config)#` **interface vlan 1**	Enters interface configuration mode, and enter the VLAN to which the IP information is assigned. VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.
Step 3	`Router(config)#` **ip address** *ip-address subnet-mask*	Enters the IP address and subnet mask.
Step 4	`Router(config)#` **exit**	Returns to global configuration mode.
Step 5	`Router#` **ip default-gateway** *ip-address*	Enters the IP address of the default router.
Step 6	`Router#` **end**	Returns to privileged EXEC mode.

Use the following procedure to remove the IP information from a switch.

Note Using the **no ip address** command in configuration mode disables the IP protocol stack and removes the IP information. Cluster members without IP addresses rely on the IP protocol stack being enabled.

Beginning in global configuration mode, follow these steps to remove an IP address.

SUMMARY STEPS

1. **`interface vlan 1`**
2. **`no ip address`**
3. **`end`**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#` **`interface vlan 1`**	Enters interface configuration mode, and enters the VLAN to which the IP information is assigned. VLAN 1 is the management VLAN, but you can configure any VLAN from IDs 1 to 1001.
Step 2	`Router(config-subif)#` **`no ip address`**	Removes the IP address and subnet mask.
Step 3	`Router(config-subif)#` **`end`**	Returns to privileged EXEC mode.

Caution If you are removing the IP address through a telnet session, your connection to the switch will be lost.

Specifying a Domain Name and Configuring the DNS

Each unique IP address can have a host name associated with it. The Cisco IOS software maintains a EC mode, and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the FTP system, for example, is identified as *ftp.cisco.com*.

To track domain names, IP has defined the concept of a domain name server (DNS), the purpose of which is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names and then specify a name server and enable the DNS, the Internet's global naming scheme that uniquely identifies network devices.

Specifying the Domain Name

You can specify a default domain name that the software uses to complete domain name requests. You can specify either a single domain name or a list of domain names. When you specify a domain name, any IP host name without a domain name has that domain name appended to it before being added to the host table.

Specifying a Name Server

You can specify up to six hosts that can function as a name server to supply name information for the DNS.

Enabling the DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The Internet's global naming scheme, the DNS, accomplishes this task. This service is enabled by default.

Enabling Switch Port Analyzer

You can monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A Switch Port Analyzer (SPAN) port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. Any number of ports can be defined as SPAN ports, and any combination of ports can be monitored. SPAN is supported for up to 2 sessions.

Beginning in privileged EXEC mode, follow these steps to enable SPAN.

SUMMARY STEPS

1. **configure terminal**
2. **monitor session** session-id {**destination** | **source**} {**interface** | **vlan** *interface-id* | *vlan-id*}} [**,** | **-** | **both** | **tx** | **rx**]
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`monitor session`** `session-id` {**`destination`** | **`source`**} {**`interface`** | **`vlan`** *`interface-id`* | *`vlan-id`*}} [**`,`** | **`-`** | **`both`** | **`tx`** | **`rx`**]	Enables port monitoring for a specific session ("*number")*. Optionally, supply a SPAN *destination* interface, and a *source* interface.
Step 3	`Router(config)#` **`end`**	Returns to privileged EXEC mode.

Beginning in privileged EXEC mode, follow these steps to disable SPAN.

SUMMARY STEPS

1. **configure terminal**
2. **no monitor session** *session-id*
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`no monitor session`** *`session-id`*	Disables port monitoring for a specific session.
Step 3	`Router(config)#` **`end`**	Returns to privileged EXEC mode.

Managing the ARP Table

To communicate with a device (on Ethernet, for example), the software first must determine the 48-bit MAC or local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses and VLAN ID. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP). By default, standard Ethernet-style ARP encapsulation (represented by the **arpa** keyword) is enabled on the IP interface.

When you manually add entries to the ARP Table by using the CLI, you must be aware that these entries do not age and must be manually removed.

Managing the MAC Address Tables

This section describes how to manage the MAC address tables on the EtherSwitch HWIC. The following topics are included:

- Understanding MAC Addresses and VLANs, page 66
- Changing the Address Aging Time, page 67
- Configuring the Aging Time, page 67
- Verifying Aging-Time Configuration, page 67

The switch uses the MAC address tables to forward traffic between ports. All MAC addresses in the address tables are associated with one or more ports. These MAC tables include the following types of addresses:

- Dynamic address—a source MAC address that the switch learns and then drops when it is not in use.
- Secure address—a manually entered unicast address that is usually associated with a secured port. Secure addresses do not age.
- Static address—a manually entered unicast or multicast address that does not age and that is not lost when the switch resets.

The address tables list the destination MAC address and the associated VLAN ID, module, and port number associated with the address. The following shows an example of a list of addresses as they would appear in the dynamic, secure, or static address table.

```
Router# show mac-address-table

Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
000a.000b.000c          Secure      1      FastEthernet0/1/8
000d.e105.cc70          Self        1      Vlan1
00aa.00bb.00cc          Static      1      FastEthernet0/1/0
```

Understanding MAC Addresses and VLANs

All addresses are associated with a VLAN. An address can exist in more than one VLAN and have different destinations in each. Multicast addresses, for example, could be forwarded to port 1 in VLAN 1 and ports 9, 10, and 11 in VLAN 5.

Each VLAN maintains its own logical address table. A known address in one VLAN is unknown in another until it is learned or statically associated with a port in the other VLAN. An address can be secure in one VLAN and dynamic in another. Addresses that are statically entered in one VLAN must be static addresses in all other VLANs.

Changing the Address Aging Time

Dynamic addresses are source MAC addresses that the switch learns and then drops when they are not in use. Use the Aging Time field to define how long the switch retains unseen addresses in the table. This parameter applies to all VLANs.

Configuring the Aging Time

Setting too short an aging time can cause addresses to be prematurely removed from the table. Then when the switch receives a packet for an unknown destination, it floods the packet to all ports in the same VLAN as the receiving port. This unnecessary flooding can impact performance. Setting too long an aging time can cause the address table to be filled with unused addresses; it can cause delays in establishing connectivity when a workstation is moved to a new port.

Beginning in global configuration mode, follow these steps to configure the dynamic address table aging time.

SUMMARY STEPS

1. **configure terminal**
2. **mac-address-table aging-time** *seconds*
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router(config)#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`mac-address-table aging-time`** *`seconds`*	Enters the number of seconds that dynamic addresses are to be retained in the address table. Valid entries are from 10 to 1000000.
Step 3	`Router(config)#` **`end`**	Returns to privileged EXEC mode.

Verifying Aging-Time Configuration

Use the **show mac-address-table aging-time** command to verify configuration:

```
Router# show mac-address-table aging-time
```

Removing Dynamic Addresses

Beginning in privileged EXEC mode, follow these steps to remove a dynamic address entry.

SUMMARY STEPS

1. **configure terminal**
2. **no mac-address-table dynamic** *hw-addr*
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`no mac-address-table dynamic`** *`hw-addr`*	Enters the MAC address to be removed from dynamic MAC address table.
Step 3	`Router(config)#` **`end`**	Returns to privileged EXEC mode.

You can remove all dynamic entries by using the **clear mac-address-table dynamic** command in privileged EXEC mode.

Verifying Dynamic Addresses

Use the **show mac-address-table dynamic** command to verify configuration:

```
Router# show mac-address-table dynamic
```

Adding Secure Addresses

The secure address table contains secure MAC addresses and their associated ports and VLANs. A secure address is a manually entered unicast address that is forwarded to only one port per VLAN. If you enter an address that is already assigned to another port, the switch reassigns the secure address to the new port.

You can enter a secure port address even when the port does not yet belong to a VLAN. When the port is later assigned to a VLAN, packets destined for that address are forwarded to the port.

Beginning in privileged EXEC mode, follow these steps to add a secure address.

SUMMARY STEPS

1. **configure terminal**
2. **mac-address-table secure address** *hw-addr* **interface** *interface-id* **vlan** *vlan-id*
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`mac-address-table secure address`** *`hw-addr`* **`interface`** *`interface-id`* **`vlan`** *`vlan-id`*	Enters the MAC address, its associated port, and the VLAN ID.
Step 3	`Router(config)#` **`end`**	Returns to privileged EXEC mode.

Beginning in privileged EXEC mode, follow these steps to remove a secure address.

SUMMARY STEPS

1. **`configure terminal`**
2. **`no mac-address-table secure`** *`hw-addr`* **`vlan`** *`vlan-id`*
3. **`end`**

DETAILED STEPS

	Command	Purpose
Step 1	`Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	`Router(config)#` **`no mac-address-table secure`** *`hw-addr`* **`vlan`** *`vlan-id`*	Enters the secure MAC address, its associated port, and the VLAN ID to be removed.
Step 3	`Router(config)#` **`end`**	Returns to privileged EXEC mode.

You can remove all secure addresses by using the **clear mac-address-table secure** command in privileged EXEC mode.

Verifying Secure Addresses

Use the **show mac-address-table secure** command to verify configuration:

```
Router# show mac-address-table secure
```

Configuring Static Addresses

A static address has the following characteristics:

- It is manually entered in the address table and must be manually removed.
- It can be a unicast or multicast address.
- It does not age and is retained when the switch restarts.

Because all ports are associated with at least one VLAN, the switch acquires the VLAN ID for the address from the ports that you select on the forwarding map. A static address in one VLAN must be a static address in other VLANs. A packet with a static address that arrives on a VLAN where it has not been statically entered is flooded to all ports and not learned.

Beginning in privileged EXEC mode, follow these steps to add a static address.

SUMMARY STEPS

1. **configure terminal**
2. **mac-address-table static** *hw-addr* [**interface**] *interface-id* [**vlan**] *vlan-id*
3. **end**

DETAILED STEPS

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **mac-address-table static** *hw-addr* [**interface**] *interface-id* [**vlan**] *vlan-id*	Enters the static MAC address, the interface, and the VLAN ID of those ports.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.

Beginning in privileged EXEC mode, follow these steps to remove a static address.

SUMMARY STEPS

1. **configure terminal**
2. **no mac-address-table static** *hw-addr* [**interface**] *interface-id* [**vlan**] *vlan-id*
3. **end**

DETAILED STEPS

:

	Command	Purpose
Step 1	Router# **configure terminal**	Enters global configuration mode.
Step 2	Router(config)# **no mac-address-table static** *hw-addr* [**interface**] *interface-id* [**vlan**] *vlan-id*	Enters the static MAC address, the interface, and the VLAN ID of the port to be removed.
Step 3	Router(config)# **end**	Returns to privileged EXEC mode.

You can remove all secure addresses by using the **clear mac-address-table static** command in privileged EXEC mode.

Verifying Static Addresses

Use the **show mac-address-table static** command to verify configuration:

```
Router # show mac-address-table static
Static Address Table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
000a.000b.000c          Static        1     FastEthernet0/1/0
```

Clearing all MAC Address Tables

To remove all addresses, use the **clear mac-address** command in privileged EXEC mode:

Command	Purpose
`Router# clear mac-address-table`	Enters to clear all MAC address tables.

Configuration Examples for EtherSwitch HWICs

This section provides the following configuration examples:

- Range of Interface: Examples, page 71
- Optional Interface Feature: Examples, page 72
- Stacking: Example, page 72
- VLAN Configuration: Example, page 73
- VLAN Trunking Using VTP: Example, page 73
- Spanning Tree: Examples, page 74
- MAC Table Manipulation: Example, page 76
- Switched Port Analyzer (SPAN) Source: Examples, page 77
- IGMP Snooping: Example, page 77
- Storm-Control: Example, page 79
- Ethernet Switching: Examples, page 79

Range of Interface: Examples

- Single Range Configuration Example, page 71
- Range Macro Definition Example, page 72

Single Range Configuration Example

The following example shows all Fast Ethernet interfaces on an HWIC-4ESW in slot 2 being reenabled:

```
Router(config)#int range fastEthernet 0/3/0 - 8
Router(config-if-range)#no shut
Router(config-if-range)#
*Mar  21 14:01:21.474: %LINK-3-UPDOWN: Interface FastEthernet0/3/0, changed state to up
*Mar  21 14:01:21.490: %LINK-3-UPDOWN: Interface FastEthernet0/3/1, changed state to up
*Mar  21 14:01:21.502: %LINK-3-UPDOWN: Interface FastEthernet0/3/2, changed state to up
*Mar  21 14:01:21.518: %LINK-3-UPDOWN: Interface FastEthernet0/3/3, changed state to up
*Mar  21 14:01:21.534: %LINK-3-UPDOWN: Interface FastEthernet0/3/4, changed state to up
*Mar  21 14:01:21.546: %LINK-3-UPDOWN: Interface FastEthernet0/3/5, changed state to up
*Mar  21 14:01:21.562: %LINK-3-UPDOWN: Interface FastEthernet0/3/6, changed state to up
*Mar  21 14:01:21.574: %LINK-3-UPDOWN: Interface FastEthernet0/3/7, changed state to up
*Mar  21 14:01:21.590: %LINK-3-UPDOWN: Interface FastEthernet0/3/8, changed state to up
Router(config-if-range)#
```

Range Macro Definition Example

The following example shows an interface-range macro named enet_list being defined to select Fast Ethernet interfaces 0/1/0 through 0/1/3:

```
Router(config)#define interface-range enet_list fastethernet 0/1/0 - 0/1/3

Router(config)#
```

The following example shows how to change to the interface-range configuration mode using the interface-range macro enet_list:

```
Router(config)#interface range macro enet_list
```

Optional Interface Feature: Examples

- Interface Speed Example, page 72
- Setting the Interface Duplex Mode Example, page 72
- Adding a Description for an Interface Example, page 72

Interface Speed Example

The following example shows the interface speed being set to 100 Mbps on Fast Ethernet interface 0/3/7:

```
Router(config)#interface fastethernet 0/3/7

Router(config-if)# speed 100
```

Setting the Interface Duplex Mode Example

The following example shows the interface duplex mode being set to full on Fast Ethernet interface 0/3/7:

```
Router(config)#interface fastethernet 0/3/7

Router(config-if)#duplex full
```

Adding a Description for an Interface Example

The following example shows how to add a description of Fast Ethernet interface 0/3/7:

```
Router(config)#interface fastethernet 0/3/7
Router(config-if)#description Link to root switch
```

Stacking: Example

The following example shows how to stack two HWICs.

```
Router(config)#interface FastEthernet 0/1/8
Router(config-if)#no shutdown
Router(config-if)#switchport stacking-partner interface FastEthernet 0/3/8
Router(config-if)#interface FastEthernet 0/3/8
Router(config-if)#no shutdown
```

Note In practice, the command **switchport stacking-partner interface FastEthernet** *0/partner-slot/partner-port* needs to be executed for only one of the stacked ports. The other port will be automatically configured as a stacking port by the Cisco IOS software. The command **no shutdown**, however, must be executed for both of the stacked ports.

VLAN Configuration: Example

The following example shows how to configure inter-VLAN routing:

```
Router#vlan database
Router(vlan)#vlan 1
Router(vlan)#vlan 2
Router(vlan)#exit
Router#configure terminal
Router(config)#interface vlan 1
Router(config-if)#ip address 1.1.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#interface vlan 2
Roouter(config-if)#ip address 2.2.2.2 255.255.255.0
Router(config-if)#no shut
Router(config-if)#interface FastEthernet 0/1/0
Router(config-if)#switchport access vlan 1
Router(config-if)#interface Fast Ethernet 0/1/1
Router(config-if)#switchport access vlan 2
Router(config-if)#exit
```

VLAN Trunking Using VTP: Example

The following example shows how to configure the switch as a VTP server:

```
Router# vlan database
Router(vlan)# vtp server
Setting device to VTP SERVER mode.
Router(vlan)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Router(vlan)# vtp password WATER
Setting device VLAN database password to WATER.
Router(vlan)# exit
APPLY completed.
Exiting....
Router#
```

The following example shows how to configure the switch as a VTP client:

```
Router# vlan database
Router(vlan)# vtp client
Setting device to VTP CLIENT mode.
Router(vlan)# exit

In CLIENT state, no apply attempted.
Exiting....
Router#
```

The following example shows how to configure the switch as VTP transparent:

```
Router# vlan database
Router(vlan)# vtp transparent
Setting device to VTP TRANSPARENT mode.
```

```
Router(vlan)# exit
APPLY completed.
Exiting....
Router#
```

Spanning Tree: Examples

Spanning-Tree Interface and Spanning-Tree Port Priority Example

The following example shows the VLAN port priority of an interface being configured:

```
Router# configure terminal
Router(config)# interface fastethernet 0/3/2
Router(config-if)# spanning-tree vlan 20 port-priority 64
Router(config-if)# end
Router#
```

The following example shows how to verify the configuration of VLAN 200 on the interface when it is configured as a trunk port:

```
Router# show spanning-tree vlan 20

 VLAN20 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 00ff.ff90.3f54
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 00ff.ff10.37b7
  Root port is 33 (FastEthernet0/3/2), cost of root path is 19
  Topology change flag not set, detected flag not set
  Number of topology flags 0 last change occurred 00:05:50 ago
  Times: hold 1, topology change 35, notification 2
     hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 0

 Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding
  Port path cost 18, Port priority 64, Port Identifier 64.33
  Designated root has priority 32768, address 00ff.ff10.37b7
  Designated bridge has priority 32768, address 00ff.ff10.37b7
  Designated port id is 128.13, designated path cost 0
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 1, received 175
Router#
```

Spanning-Tree Port Cost Example

The following example shows how to change the spanning-tree port cost of a Fast Ethernet interface:

```
Router# configure terminal
Router(config)# interface fastethernet 0/3/2
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
Router#

Router#show run interface fastethernet0/3/2
Building configuration...

Current configuration: 140 bytes
!
interface FastEthernet0/3/2
 switchport access vlan 20
  no ip address
  spanning-tree vlan 20 port-priorityy 64
  spanning-tree cost 18
end
```

The following example shows how to verify the configuration of the interface when it is configured as an access port:

```
Router# show spanning-tree interface fastethernet 0/3/2
 Port 33 (FastEthernet0/3/2) of VLAN20 is forwarding
  Port path cost 18, Port priority 64, Port Identifier 64.33
  Designated root has priority 32768, address 00ff.ff10.37b7
  Designated bridge has priority 32768, address 00ff.ff10.37b7
  Designated port id is 128.13, designated path cost 0
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 1, received 175
Router#
```

Bridge Priority of a VLAN

The following example shows the bridge priority of VLAN 20 being configured to 33792:

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 priority 33792
Router(config)# end
Router#
```

Hello Time Example

The following example shows the hello time for VLAN 20 being configured to 7 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 hello-time 7
Router(config)# end
Router#
```

Forward-Delay Time for a VLAN Example

The following example shows the forward delay time for VLAN 20 being configured to 21 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 forward-time 21
Router(config)# end
Router#
```

Maximum Aging Time for a VLAN Example

The following example configures the maximum aging time for VLAN 20 to 36 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 max-age 36
Router(config)# end
Router#
```

Spanning Tree Examples

The following example shows spanning tree being enabled on VLAN 20:

```
Router# configure terminal
Router(config)# spanning-tree vlan 20
Router(config)# end
Router#
```

Note Because spanning tree is enabled by default, issuing a show running command to view the resulting configuration will not display the command you entered to enable spanning tree.

The following example shows spanning tree being disabled on VLAN 20:

```
Router# configure terminal
Router(config)# no spanning-tree vlan 20
Router(config)# end
Router#
```

Spanning Tree Root Example

The following example shows the switch being configured as the root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
Router#
```

MAC Table Manipulation: Example

The following example shows a static entry being configured in the MAC address table:

```
Router(config)# mac-address-table static beef.beef.beef int fa0/1/5
Router(config)# end
```

The following example shows port security being configured in the MAC address table.

```
Router(config)# mac-address-table secure 0000.1111.2222 fa0/1/2 vlan 3
Router(config)# end
```

Switched Port Analyzer (SPAN) Source: Examples

SPAN Source Configuration Example

The following example shows SPAN session 1 being configured to monitor bidirectional traffic from source interface Fast Ethernet 0/1/1:

```
Router(config)# monitor session 1 source interface fastethernet 0/1/1
```

SPAN Destination Configuration Example

The following example shows interface Fast Ethernet 0/3/7 being configured as the destination for SPAN session 1:

```
Router(config)# monitor session 1 destination interface fastethernet 0/3/7
```

Removing Sources or Destinations from a SPAN Session Example

This following example shows interface Fast Ethernet 0/3/2 being removed as a SPAN source for SPAN session 1:

```
Router(config)# no monitor session 1 source interface fastethernet 0/3/2
```

IGMP Snooping: Example

The following example shows the output from configuring IGMP snooping:

```
Router# show mac-address-table multicast igmp-snooping

HWIC Slot: 1
--------------
    MACADDR     VLANID     INTERFACES

0100.5e05.0505    1        Fa0/1/1
0100.5e06.0606    2

HWIC Slot: 3
--------------
    MACADDR     VLANID     INTERFACES

0100.5e05.0505    1        Fa0/3/4
0100.5e06.0606    2        Fa0/3/0

Router#
```

The following is an example of output from the **sh run int** privileged EXEC command for VLAN 1:

```
Router#sh run int vlan 1

Building configuration...

Current configuration :82 bytes
```

```
!
interface Vlan1
 ip address 192.168.4.90 255.255.255.0
 ip pim sparse-mode
end

Router#sh run int vlan 2

Building configuration...

Current configuration :82 bytes
!
interface Vlan2
 ip address 192.168.5.90 255.255.255.0
 ip pim sparse-mode
end

Router#
Router# sh ip igmp group

IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.255.255.255  Vlan1                    01:06:40  00:02:20  192.168.41.101
224.0.1.40       Vlan2                    01:07:50  00:02:17  192.168.5.90
224.5.5.5        Vlan1                    01:06:37  00:02:25  192.168.41.100
224.5.5.5        Vlan2                    01:07:40  00:02:21  192.168.31.100
224.6.6.6        Vlan1                    01:06:36  00:02:22  192.168.41.101
224.6.6.6        Vlan2                    01:06:39  00:02:20  192.168.31.101
Router#

Router# show ip mroute

IP Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C -
Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 239.255.255.255), 01:06:43/00:02:17, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:43/00:02:17

(*, 224.0.1.40), 01:12:42/00:00:00, RP 0.0.0.0, flags:DCL
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan2, Forward/Sparse, 01:07:53/00:02:14

(*, 224.5.5.5), 01:07:43/00:02:22, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:40/00:02:22
    Vlan2, Forward/Sparse, 01:07:44/00:02:17
```

```
(*, 224.6.6.6), 01:06:43/00:02:18, RP 0.0.0.0, flags:DC
  Incoming interface:Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan1, Forward/Sparse, 01:06:40/00:02:18
    Vlan2, Forward/Sparse, 01:06:43/00:02:16

Router#
```

Storm-Control: Example

The following example shows bandwidth-based multicast suppression being enabled at 70 percent on Fast Ethernet interface 2:

```
Router# configure terminal
Router(config)# interface FastEthernet0/3/3
Router(config-if)# storm-control multicast threshold 70.0 30.0
Router(config-if)# end

Router#show storm-control multicast
Interface  Filter State  Upper    Lower    Current
---------  ------------  -----    -----    -------
Fa0/1/0    inactive      100.00%  100.00%  N/A
Fa0/1/1    inactive      100.00%  100.00%  N/A
Fa0/1/2    inactive      100.00%  100.00%  N/A
Fa0/1/3    inactive      100.00%  100.00%  N/A
Fa0/3/0    inactive      100.00%  100.00%  N/A
Fa0/3/1    inactive      100.00%  100.00%  N/A
Fa0/3/2    inactive      100.00%  100.00%  N/A
Fa0/3/3    Forwarding     70.00%   30.00%  0.00%
Fa0/3/4    inactive      100.00%  100.00%  N/A
Fa0/3/5    inactive      100.00%  100.00%  N/A
Fa0/3/6    inactive      100.00%  100.00%  N/A
Fa0/3/7    inactive      100.00%  100.00%  N/A
Fa0/3/8    inactive      100.00%  100.00%  N/A
```

Ethernet Switching: Examples

- Subnets for Voice and Data Example, page 79
- Inter-VLAN Routing Example, page 80
- Single Subnet Configuration Example, page 80
- Ethernet Ports on IP Phones with Multiple Ports Example, page 81

Subnets for Voice and Data Example

The following example shows separate subnets being configured for voice and data on the EtherSwitch HWIC:

```
interface FastEthernet0/1/1
     description DOT1Q port to IP Phone
     switchport native vlan 50
     switchport mode trunk
     switchport voice vlan 150
```

```
interface Vlan 150
     description voice vlan
     ip address 10.150.1.1 255.255.255.0
     ip helper-address 172.20.73.14 (See Note below)

interface Vlan 50
     description data vlan
     ip address 10.50.1.1 255.255.255.0
```

This configuration instructs the IP phone to generate a packet with an 802.1Q VLAN ID of 150 with an 802.1p value of 5 (default for voice bearer traffic).

Note In a centralized CallManager deployment model, the DHCP server might be located across the WAN link. If so, an **ip helper-address** command pointing to the DHCP server should be included on the voice VLAN interface for the IP phone. This is done to obtain its IP address as well as the address of the TFTP server required for its configuration.
Be aware that IOS supports a DHCP server function. If this function is used, the EtherSwitch HWIC serves as a local DHCP server and a helper address would not be required.

Inter-VLAN Routing Example

Configuring inter-vlan routing is identical to the configuration on an EtherSwitch HWIC with an MSFC. Configuring an interface for WAN routing is consistent with other IOS platforms.

The following example provides a sample configuration:

```
interface Vlan 160
     description voice vlan
     ip address 10.6.1.1 255.255.255.0

interface Vlan 60
     description data vlan
     ip address 10.60.1.1 255.255.255.0

interface Serial0/3/0
     ip address 160.3.1.2 255.255.255.0
```

Note Standard IGP routing protocols such as RIP, IGRP, EIGRP, and OSPF are supported on the EtherSwitch HWIC. Multicast routing is also supported for PIM dense mode, sparse mode and sparse-dense mode.

Single Subnet Configuration Example

The EtherSwitch HWIC supports the use of an 802.1p-only option when configuring the voice VLAN. Using this option allows the IP phone to tag VoIP packets with a CoS of 5 on the native VLAN, while all PC data traffic is sent untagged.

The following example shows a single subnet configuration for the EtherSwitch HWIC:

```
Router# FastEthernet 0/1/2
description Port to IP Phone in single subnet
     switchport access vlan 40
```

The EtherSwitch HWIC instructs the IP phone to generate an 802.1Q frame with a null VLAN ID value but with an 802.1p value (default is COS of 5 for bearer traffic). The voice and data vlans are both 40 in this example.

Ethernet Ports on IP Phones with Multiple Ports Example

The following example illustrates the configuration for the IP phone:

```
interface FastEthernet0/x/x
     switchport voice vlan x
     switchport mode trunk
```

The following example illustrates the configuration for the PC:

```
interface FastEthernet0/x/y
     switchport mode access
     switchport access vlan y
```

Note Using a separate subnet, and possibly a separate IP address space, may not be an option for some small branch offices due to the IP routing configuration. If the IP routing can handle an additional subnet at the remote branch, you can use Cisco Network Registrar and secondary addressing.

Additional References

The following sections provide references related to EtherSwitch HWICs.

Related Documents

Related Topic	Document Title
Hardware Installation of Interface Cards	*Cisco Interface Cards Installation Guide*
Information about configuring Voice over IP features	*Cisco IOS Voice, Video, and Fax Configuration Guide*
Voice over IP commands	*Cisco IOS Voice, Video, and Fax Command Reference, Release 12.3 T*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards have not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs have not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs have not been modified by this feature.	—

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