



# 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
---------	--------------

---

## 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** the login dialog box and follow the instructions that appear.

## Contents

- 
- [Restrictions for EtherSwitch HWICs, page 2](#)
- [Information About EtherSwitch HWICs, page 2](#)
- [How to Configure EtherSwitch HWICs, page 5](#)



---

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

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

- [Additional References](#), page 71
- [Additional References](#), page 81

## Prerequisites for EtherSwitch HWICs

- [Additional References](#), page 71  
*Cisco IOS IP Configuration Guide*

## Restrictions for EtherSwitch HWICs

- 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 duplex auto**

## Information About EtherSwitch HWICs

- 
- 
- 
-

- 
- 
- [Switched Port Analyzer, page 4](#)
  - [IGMP Snooping, page 4](#)
  - [Storm Control, page 4](#)
  - [Intrachassis Stacking, page 4](#)
  - [Fallback Bridging, page 4](#)

## VLANs

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t\\_4/gt1636nm.htm#1047027](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt1636nm.htm#1047027)

## Inline Power for Cisco IP Phones

## Layer 2 Ethernet Switching

## 802.1x Authentication

## Spanning Tree Protocol

## **Cisco Discovery Protocol**

## **Switched Port Analyzer**

## **IGMP Snooping**

## **Storm Control**

## **Intrachassis Stacking**

## **Fallback Bridging**



## DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		

## Verifying the VLAN Configuration

### show

```
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
```

```
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)#
APPLY completed.
Exiting....
router#
router#
```

## show vlan-switch

### show vlan-switch

```
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

### SUMMARY STEPS

- 1.
- 2.
- 3.

### DETAILED STEPS

Router#	
Router(vlan)#	—
Router(vlan)#	

### Verifying VLAN Deletion

<output truncated>

Router(vlan)#

**show vlan-switch brief**

`switch brief`



Note

## Configuring a VTP Server

### SUMMARY STEPS

- 1.
2. `ntp server`
3. `ntp domain domain name`
4. `ntp password password value`
- 5.

### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		

	Command	Purpose
Step 3		
Step 4		
Step 5		

	Command	Purpose
Step 1		
Step 2		
Step 3		

**Disabling VTP (VTP Transparent Mode)**

**SUMMARY STEPS**

- 1.
- 2.
- 3.

## DETAILED STEPS

Router#	
Router(vlan) #	
Router(vlan) #	

## Verifying VTP

```
show vtp status
```

```
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 a Range of Interfaces

### interface range

```
Router(config)# { macro_name
FastEthernet interface-id [ interface-id ] |
vlan_ID} [, FastEthernet [ -
] | vlan vlan_ID
```

0/<slot>/0 -

**3** is valid; the command **interface range fastethernet 0/< >/0-0/< >/3** 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 **interface range** command only supports VLAN interfaces that are configured with the **interface vlan** command.

### define interface range

```
macro_name
interface-id interface-id
vlan_ID vlan_ID interface-id
interface-id
```

## Verifying Configuration of an Interface Range Macro

```
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

- 
- 
- 



Caution

### Configuring the Interface Speed

#### SUMMARY STEPS

- 1.
2. `speed 10 100 auto`

<code>interface fastethernet</code>	Selects the interface to be configured.
<code>speed 10 100 auto</code>	Sets the interface speed of the interface.



```
interface fastethernet
duplex [auto | full | half]
```

Router(config)#	Selects the interface to be configured.
Router(config-if)#	Sets the duplex mode of the interface.



```
interface fastethernet 0/1/0
speed 100
duplex auto
end
```

```
show interfaces fastethernet 0/1/0
```

```
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#

```

Command	Purpose
<i>string</i>	

## Configuring a Fast Ethernet Interface as a Layer 2 Trunk

### SUMMARY STEPS

- 1.
- 2.
3. `trunk`
4. `switchport trunk native vlan`
5. `switchport trunk allowed vlan add except none remove vlan1 vlan vlan ...`
- 6.
- 7.

### DETAILED STEPS

<i>interface-id</i>	
<i>vlan-num</i>	(Optional) For 802.1Q trunks, specifies the native 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.

Router(config-if)#	
Router(config-if)#	



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

```
show running-config interfaces fastEthernet 0/3/1
```

```
!  
interface FastEthernet0/3/1  
    switchport mode trunk  
    no ip address  
end  
router#  
  
router#  
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#
```

<code>interface fastethernet</code>	
<code>shutdown</code>	
<code>switchport mode access</code>	
<code>switchport access vlan</code>	
<code>no shutdown</code>	
<code>end</code>	

### Verifying a Fast Ethernet Interface as Layer 2 Access

t 0/1/2

```
show interfaces f0/1/0 switchport
```

## Understanding the Default 802.1x Configuration

**Table 1**     *Default 802.1x Configuration*

<b>Feature</b>	<b>Default Setting</b>
<ul style="list-style-type: none"><li>•</li><li>•</li><li>• Key</li></ul>	<ul style="list-style-type: none"><li>• None specified.</li><li>• 1645.</li><li>• None specified.</li></ul>
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.

**Default 802.1x Configuration (continued)**


**802.1x Configuration Guidelines**

- 
- 
- 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****SUMMARY STEPS**

- 1.
  - 2.
  3. `method1 method2`
- `interface-id`

8. `copy running-config startup-config`

	Command	Purpose
Step 1		
Step 2		
Step 3		<ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul>
Step 4		
Step 5		<p style="text-align: right;"><a href="#">“802.1x Configuration Guidelines” section on page 19.</a></p>
		Returns to privileged EXEC mode.
		Verifies your entries. Check the Status column in the 802.1x Port Summary section of the display. An <i>enabled</i>

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

## Configuring the Switch-to-RADIUS-Server Communication

*port-number string*

	<i>ip-address,</i>
	<b>auth-port</b> <i>port-number</i>
	<b>key</b> <i>string</i>
	<b>host</b>
	<b>radius-server</b>

*ip-address*

**radius-server key**



	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>		
<b>Step 2</b>		
<b>Step 3</b>		
<b>Step 4</b>		
<b>Step 5</b>		
<b>Step 6</b>		

**no dot1x re-authentication**

**no**

**dot1x timeout re-authperiod**

## **Changing the Quiet Period**



**SUMMARY STEPS**

- 1.
2. `quiet-period`  
`end`  
`show dot1x`  
`copy running-config startup-config`

	Enters global configuration mode.
	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.
	Returns to privileged EXEC mode.
	Verifies your entries.
	(Optional) Saves your entries in the configuration file.

**dot1x timeout quiet-period**

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:

	Enters global configuration mode.
	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.
	Returns to privileged EXEC mode.
	Verifies your entries.
	(Optional) Saves your entries in the configuration file.

To return to the default retransmission time, use the `no eap-retransmit` global configuration command.

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.



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:

	Enters global configuration mode.
	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.
	Returns to privileged EXEC mode.

	Command	Purpose
Step 4		
Step 5		

To return to the default retransmission number, use the `global configuration` command.

## Enabling Multiple Hosts

### SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

# Resetting the 802.1x Configuration to the Default Values

## SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.

## DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

## Displaying 802.1x Statistics and Status

# Configuring Spanning Tree

- 
- 
- 
- 
- 
- 
- 
-

## Enabling Spanning Tree

<i>vlan ID</i>	

## Verifying Spanning Tree

## Configuring Spanning Tree Port Priority

### SUMMARY STEPS

- 1.
2. `vlan ID priority port priority`

interface ethernet fastethernet	
no spanning tree port priority	
no spanning tree vlan port priority	
end	

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

```
interface ethernet fastethernet
no spanning tree cost
no spanning tree vlan cost
end
```

fastethernet	interface ethernet
	no spanning tree cost
cost	no spanning tree vlan
	end

	Default Cost Value

Port Speed	Recommended Value	Recommended Range

show spanning tree vlan 200

## Configuring the Bridge Priority of a VLAN

Command	Purpose
	no



Caution

spanning-tree vlan vlan ID root secondary

ID root primary

## Verifying the Bridge Priority of a VLAN

show spanning tree vlan bridge

## Configuring the Hello Time

Command	Purpose
	hello time
	no

## Configuring the Forward-Delay Time for a VLAN

Command	Purpose
	<code>forward time</code> <code>no</code>

## Configuring the Maximum Aging Time for a VLAN

Command	Purpose
<code>max age</code>	

## Configuring the Root Bridge



Note

---

---



Command	Purpose

Command	Purpose

Verifying that Spanning Tree is Disabled.

## Configuring MAC Table Manipulation

- 
- 
- 
- 

## Enabling Known MAC Address Traffic

### SUMMARY STEPS

- 1.
- 2.
- 3.

**DETAILED STEPS**

	<b>Command</b>	<b>Purpose</b>
Step 1		
Step 2		
Step 3		

**Verifying the MAC Address Table Secure Option****Creating a Static Entry in the MAC Address Table****SUMMARY STEPS**

- 1.
- 2.
- 3.

**DETAILED STEPS**

	<b>Command</b>	<b>Purpose</b>
Step 1		
Step 2		
Step 3		

**Verifying the Mac Address Table**

## Configuring the Aging Timer

### SUMMARY STEPS

- 1.
- 2.
- 3.

### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		



Caution

## Verifying the Aging Time

## Configuring Cisco Discovery Protocol

- 
- 
-

## Enabling Cisco Discovery Protocol

Command	Purpose

### Verifying the CDP Global Configuration

## Enabling CDP on an Interface

Command	Purpose

### Verifying the CDP Interface Configuration

### Verifying CDP Neighbors

### Monitoring and Maintaining CDP

Command	Purpose

### Configuring the Switched Port Analyzer (SPAN)

  
Note

\_\_\_\_\_

\_\_\_\_\_

  
Note

\_\_\_\_\_

\_\_\_\_\_

- 
- 
- 
- 

### Configuring the SPAN Sources

Command	Purpose

## Configuring SPAN Destinations

Command	Purpose
<pre>Router(config)# {     } [,   -]   {     _ID}}</pre>	

## Verifying the SPAN Session

```

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

Command	Purpose
<pre>Router(config)#</pre>	

## Configuring Power Management on the Interface

### SUMMARY STEPS

- 1.
- 2.
3. /

## DETAILED STEPS

	Command	Purpose
Step 1	Router#	
Step 2	Router(config)#	
Step 3	Router(config-if)# /	<b>Note</b>

## Verifying Power Management on the Interface

Router#

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

Router# [ | ]

---

## Configuring IP Multicast Layer 3 Switching

- 
- 
- 
- 

### Enabling IP Multicast Routing Globally

- 
- *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services*

*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*

*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*

Command	Purpose

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

#### SUMMARY STEPS

- 1.
- 2.



## DETAILED STEPS

Router(config)#	
Router(config-if)#	{
	}

## Verifying IP Multicast Layer 3 Hardware Switching Summary



## Note

## Step 1

```

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#

Router#

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#

```



```
Router#  
  
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 unreachable 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#
```

```
Router# show ip mroute 224.10.103.10
```

```
  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#



[Statically Configuring an Interface to Join a Group, page 44](#)

[Configuring a Multicast Router Port, page 45](#)

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.

	Enters global configuration mode.
	Globally enables IGMP snooping in all existing VLAN interfaces.
	Returns to privileged EXEC mode.

	Displays snooping configuration.
	(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.

[ ]

	Enters global configuration mode.
	Enables IGMP snooping on the VLAN interface.
	Returns to privileged EXEC mode.
]	Displays snooping configuration. (Optional) is the number of the VLAN.
	(Optional) Saves your configuration to the startup configuration.

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

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.

	Command	Purpose
Step 1		
Step 2		
Step 3		

To disable Immediate-Leave processing, follow Steps 1 and 2 to enter interface configuration mode, and use the global configuration command.

## Statically Configuring an Interface to Join a Group

### SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.

### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li></ul>
Step 3		

	Command	Purpose
Step 4		<ul style="list-style-type: none"> <li>•</li> <li>•</li> <li>•</li> <li>•</li> </ul>
Step 5		

## Configuring a Multicast Router Port

### SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

## Configuring Per-Port Storm-Control

- 
- 

### Enabling Per-Port Storm-Control

#### SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

#### DETAILED STEPS

	Command	Purpose
Step 1		Enters global configuration mode.
Step 2		Enters interface configuration mode, and enter the port to configure.
Step 3		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		Selects the                    keyword to disable the port during a storm. The default is to filter out the traffic.
Step 5		Returns to privileged EXEC mode.
Step 6		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.
- 2.
- 3.
- 4.
- 5.
- 6.

### DETAILED STEPS

	Command	Purpose
Step 1		Enters global configuration mode.
Step 2		Enters interface configuration mode, and enter the port to configure.
Step 3		Disables per-port storm control.
Step 4		Disables the specified storm control action.
Step 5		Returns to privileged EXEC mode.
Step 6		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.
- 2.
- 3.

- 4.
- 5.
- 6.
- 7.

## DETAILED STEPS

	Command	Purpose
Step 1		Selects the interface to configure.
Step 2		Activates the interface. (Required only if you shut down the interface.)
Step 3		Selects and configures the stacking partner port. To restore the defaults, use the form of this command.
Step 4		Exits interface configuration mode.
Step 5		Selects the stacking partner interface.
Step 6		Activates the stacking partner interface.
Step 7		Exits configuration mode.



### Note

Both stacking partner ports must have their and parameters set to .



### Caution

If stacking is removed, stacked interfaces will go to 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

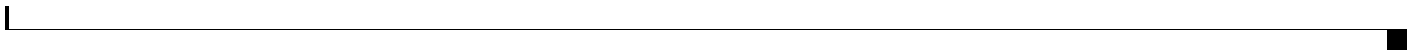
### *Default Fallback Bridging Configuration*

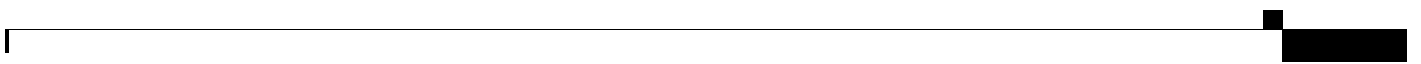

## Creating a Bridge Group

### SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.






	<i>bridge-group</i>
	<i>mac-address</i>
	<i>interface-id</i>

## Adjusting Spanning-Tree Parameters

- 
- 
- 
- 
- 



**Note**

*Configuration Fundamentals Command Reference*

## Changing the Switch Priority

### SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.

### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"><li>•</li><li>•</li></ul>
Step 3		
Step 4		
Step 5		

## Changing the Interface Priority

### SUMMARY STEPS

- 1.
- 2.
- 3.

- 4.
- 5.
- 6.

## DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		<ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul>
Step 4		
Step 5		
Step 6		

## Assigning a Path Cost

## SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.

DETAILED STEPS

Command	Purpose
Step 1	
Step 2	
Step 3	<ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul>
Step 4	
Step 5	
Step 6	

Adjusting BPDUs Intervals

- 
- 
- 



Note

Adjusting the Interval between Hello BPDUs

SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.

**DETAILED STEPS**

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul>
Step 3		
Step 4		
Step 5		

**Changing the Forward-Delay Interval****SUMMARY STEPS**

- 1.
- 2.
- 3.
- 4.
- 5.

**DETAILED STEPS**

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul>
Step 3		
Step 4		
Step 5		

### Changing the Maximum-Idle Interval

#### SUMMARY STEPS

- 1.
- 2.
- 3.
- 4.
- 5.

#### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul>
Step 3		
Step 4		
Step 5		

### Disabling the Spanning Tree on an Interface

#### SUMMARY STEPS

- 1.
- 2.

- 3.
- 4.
- 5.
- 6.

## DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

## Monitoring and Maintaining the Network

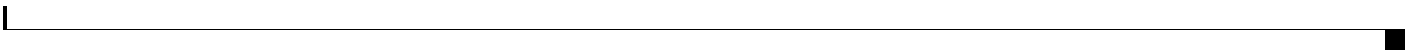
Command	Purpose

## Configuring Separate Voice and Data Subnets



**Note**

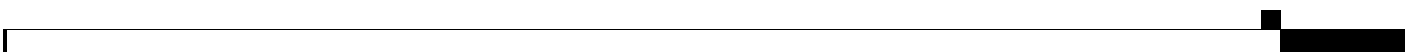
*Cisco AVVID QoS Design Guide*

	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>		
<b>Step 2</b>		
<b>Step 3</b>		
<b>Step 4</b>		

## **Managing the EtherSwitch HWIC**

- 
- 
- 



- 
- 
- 
- 
- 
- 

### Adding Trap Managers

#### SUMMARY STEPS

- 1.
2. `snmp-server host 172.2.128.263 snmp vlan-membership`  
`end`

<code>configure terminal</code>	
<code>snmp-server host 172.2.128.263 snmp vlan-membership</code>	
<code>end</code>	

`show running-config`

## Assigning IP Information to the Switch

### SUMMARY STEPS

- 1.
- 2.
3. `ip-address subnet-mask`

`ip-address`

<code>subnet-mask</code>	<code>ip-address</code>	
	<code>ip-address</code>	



---

---



	Command	Purpose
Step 1		
Step 2		
Step 3		



---

---

*cisco.com*

*ftp.cisco.com*

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**

**Specifying a Name Server**



Enabling the DNS

Enabling Switch Port Analyzer

SUMMARY STEPS

- 1.
- 2.
- 3.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		<i>destination</i> <i>number</i> ”).
		<i>source</i>

SUMMARY STEPS

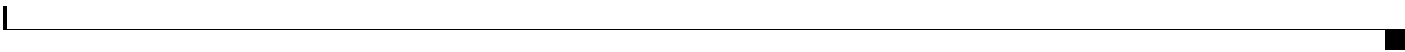
- 1.
- 2.
- 3.

DETAILED STEPS


---

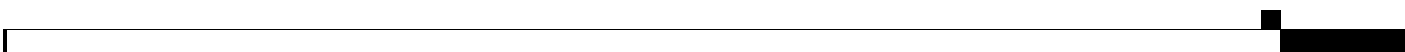
*address resolution*

---



	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>		
<b>Step 2</b>		
<b>Step 3</b>		

**Verifying Aging-Time Configuration**



## Removing Dynamic Addresses

### SUMMARY STEPS

- 1.
- 2.
- 3.

### DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		
Step 3		

### Verifying Dynamic Addresses

## Adding Secure Addresses

### SUMMARY STEPS

- 1.
- 2.
- 3.

**DETAILED STEPS**

	Enters global configuration mode.
	Enters the MAC address, its associated port, and the VLAN ID.
	Returns to privileged EXEC mode.

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

	Enters global configuration mode.
	Enters the secure MAC address, its associated port, and the VLAN ID to be removed.
	Returns to privileged EXEC mode.

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

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

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.

	Enters global configuration mode.
-	Enters the static MAC address, the interface, and the VLAN ID of those ports.
	Returns to privileged EXEC mode.

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

	Enters global configuration mode.
-	Enters the static MAC address, the interface, and the VLAN ID of the port to be removed.
	Returns to privileged EXEC mode.

You can remove all secure addresses by using the `no mac-address` command in privileged EXEC mode.

Use the `show mac-address` command to verify configuration:

## Clearing all MAC Address Tables

Command	Purpose
Router#	

## Configuration Examples for EtherSwitch HWICs

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

### Range of Interface: Examples

- 
- 

### Single Range Configuration Example

```
*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

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

```
interface range macro enet list
```

## Optional Interface Feature: Examples

- 
- 
- 

## Interface Speed Example

## Setting the Interface Duplex Mode Example

## Adding a Description for an Interface Example

```
description Link to root switch
```

```
interface FastEthernet 0/1/8
no shutdown
switchport stacking-partner interface FastEthernet 0/3/8
interface FastEthernet 0/3/8
no shutdown
```



---

```
switchport stacking-partner interface FastEthernet  
0/partner-slot/partner-port
```

---

```
ip address 1.1.1.1 255.255.255.0  
no shut  
interface vlan 2  
ip address 2.2.2.2 255.255.255.0  
no shut  
interface FastEthernet 0/1/0  
switchport access vlan 1  
interface Fast Ethernet 0/1/1  
switchport access vlan 2  
exit
```

## VLAN Trunking Using VTP: Example

Network

```
vtp password WATER  
exit
```

```
vlan database  
vtp client  
exit
```

```
vlan database  
vtp transparent
```

---

exit

```
configure terminal
  interface fastethernet 0/3 2
    spanning tree vlan 20 port priority 64
  end
```

```
show spanning tree vlan 20
```

---

```
configure terminal
  interface fastethernet 0/3/2
    spanning tree cost 18
  end
```

```
show run interface fastethernet0/3/2
```

```
show spanning tree interface fastethernet 0/3/2
```

```
configure terminal
  spanning tree vlan 20 priority 33792
end
```

```
configure terminal
  spanning tree vlan 20 hello-time 7
end
```

```
configure terminal
  spanning tree vlan 20 forward-time 21
end
```

```
configure terminal
  spanning tree vlan 20 max age 36
end
```

```
configure terminal
  spanning tree vlan 20
end
```



```
configure terminal
  no spanning tree vlan 20
end
```

```
configure terminal
  spanning tree vlan 10 root primary diameter 4
exit
```

```
mac-address-table static beef.beef.beef int fa0/1/5
end
```

```
mac-address-table secure 0000.1111.2222 fa0/1/2 vlan 3
end
```

---

```
monitor session 1 source interface fastethernet 0/1 1
```

```
monitor session 1 destination interface fastethernet 0/3/7
```

```
no monitor session 1 source interface fastethernet 0/3/2
```

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

```
sh run int vlan 1
```

---


---

sh run int vlan 2

sh ip igmp group

show ip mroute

---



---

```
configure terminal
  interface FastEthernet0/3/3
    storm-control multicast threshold 70.0 30.0
  end

show storm-control multicast
```

---

Note



---

---



---

---

FastEthernet 0/1/2



## Additional References

## Related Documents

Related Topic	Document Title
	<a href="#">Cisco IOS Voice, Video, and Fax Configuration Guide</a>
	<a href="#">Cisco IOS Voice, Video, and Fax Command Reference, Release 12.3 T</a>

## Standards


MIBs	MIBs Link

RFCs	Title

Description	Link

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.