

Configuring the Ethernet Switches

This chapter gives an overview of configuration tasks for the 4-port Fast Ethernet (FE) switch, and for the Gigabit Ethernet (GE) switch that services the embedded wireless access point on the Cisco 860 and Cisco 880 series Integrated Services Routers (ISRs).

The FE switches are 10/100Base T Layer 2 Fast Ethernet switches. Traffic between different VLANs on a switch is routed through the router platform with the switched virtual interface (SVI).

The GE switch is a 1000Base T Layer 2 Gigabit Ethernet switch, the internal interface between the router and its embedded wireless access point.

Any switch port may be configured as a trunking port to connect to other Cisco Ethernet switches.

An optional power module can be added to Cisco 880 series ISRs to provide inline power to two of the FE ports for IP telephones or external access points.

This chapter contains the following sections:

-
-
-
- [How to Configure Ethernet Switches, page 6-4](#)

Switch Port Numbering and Naming

The ports on the FE switch are numbered FE0 through FE3. The port on the GE switch is named and numbered Wlan-GigabitEthernet0.

Restrictions for the FE Switch

- The ports of an FE switch must NOT be connected to any Fast Ethernet onboard port of the router.
- On Cisco 880 series ISRs, inline power is supported only on FE switch ports FE0 and FE1. Inline power is not supported on Cisco 860 series ISRs.
- VTP pruning is not supported.
- The FE switch can support up to 200 secure MAC addresses.

Information About Ethernet Switches

-
-
-
-
-
- Cisco Discovery Protocol, page 6-3
- Switched Port Analyzer, page 6-3
- IGMP Snooping, page 6-3
- Storm Control, page 6-4
- Fallback Bridging, page 6-4

VLANs and VLAN Trunk Protocol

For information on the concepts of VLANs and VLAN Trunk Protocol (VTP), see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1047027

Inline Power

Inline power is not supported on the Cisco 860 series ISRs. On the Cisco 880 series ISRs, inline power can be supplied to Cisco IP phones or external access points on FE switch ports FE0 and FE1.

A detection mechanism on the FE switch determines whether it is connected to a Cisco device. If the switch senses that there is no power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch to never supply power to the Cisco device and to disable the detection mechanism.

The FE switch also provides support for powered devices compliant with IEEE 802.3af.

Layer 2 Ethernet Switching

For information on the concept of Layer 2 Ethernet Switching, see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1048478

802.1x Authentication

For information on the concept of 802.1x Authentication, see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1051006

Spanning Tree Protocol

For information on the concept of Spanning Tree Protocol, see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1048458

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all LAN and WAN media that support Subnetwork Access Protocol (SNAP). Each CDP-configured device sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain the time-to-live, or hold-time information, which indicates the length of time a receiving device should hold CDP information before discarding it.

Switched Port Analyzer

For information on the concept of Switched Port Analyzer, see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1053663

IGMP Snooping

For information on the concept of IGMP Snooping, see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1053727

IGMP Version 3

The Cisco 880 series ISRs support Version 3 of IGMP snooping.

IGMPv3 provides supports for source filtering, which enables a multicast receiver host to signal to a router which groups the receiver host wants to receive multicast traffic from, and from which sources this traffic is expected. Enabling the IGMPv3 feature with IGMP snooping on Cisco ISRs provides Basic IGMPv3 Snooping Support (BISS). BISS provides constrained flooding of multicast traffic in the presence of IGMPv3 hosts. This support constrains traffic to approximately the same set of ports as IGMPv2 snooping does with IGMPv2 hosts. The constrained flooding only considers the destination multicast address.

Storm Control

For information on the concept of storm control, see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1051018

Fallback Bridging

For information on the concept of fallback bridging, see the information at this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1054833

How to Configure Ethernet Switches

See the following sections for configuration tasks for Ethernet switches.

- [Configuring VLANs, page 6-4](#)
- [Configuring Layer 2 Interfaces, page 6-6](#)
- [Configuring 802.1x Authentication, page 6-6](#)
- [Configuring Spanning Tree Protocol, page 6-6](#)
- [Configuring MAC Table Manipulation, page 6-7](#)
- [Configuring Cisco Discovery Protocol, page 6-7](#)
- [Configuring the Switched Port Analyzer, page 6-7](#)
- [Configuring Power Management on the Interface, page 6-8](#)
- [Configuring IP Multicast Layer 3 Switching, page 6-8](#)
- [Configuring IGMP Snooping, page 6-8](#)
- [Configuring Per-Port Storm Control, page 6-9](#)
- [Configuring Fallback Bridging, page 6-9](#)
- [Configuring Separate Voice and Data Subnets, page 6-9](#)
- [Managing the Switch, page 6-10](#)

Configuring VLANs

This section provides information on how to configure VLANs. The Cisco 860 series ISRs support 2 VLANs. and the Cisco 880 series ISRs support 8 VLANs.

- [VLANs on the FE Ports, page 6-4](#)
- [VLANs on the GE Port, page 6-5](#)

VLANs on the FE Ports

Perform these steps to configure VLANs, beginning in configuration mode.

	Command	Purpose
Step 1	<code>interface fe <i>port</i></code>	
Step 2	<code>shutdown</code>	
Step 3	<code>switchport</code>	<p>Note</p> <p><code>switchport</code></p> <p><code>switchport mode dynamic desirable negotiate</code></p>
Step 4	<code>switchport access vlan <i>vlan_id</i></code>	<i>vlan_id</i>
Step 5	<code>no shutdown</code>	
Step 6	<code>end</code>	

For additional information, see the information at the following URL:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html>

VLANs on the GE Port

Because the GE port is an internal interface that services only the router's embedded access point, it cannot be configured only with the command `switchport access vlan X`, where X is other than 1. It may, however, be configured in trunk mode. This may be done by performing the following steps, beginning in configuration mode.

	Comand	Purpose
Step 1	<code>interface <i>Wlan-GigabitEthernet0</i></code>	
Step 1	<code>switchport mode trunk</code>	
Step 1	<code>switchport access vlan <i>vlan_id</i></code>	

Configuring Layer 2 Interfaces

-
-
-

Configuring 802.1x Authentication

-
-
-
-
-
-
-
-
-
-

Configuring Spanning Tree Protocol

-
-
-
-
-
-
-
-
-

Configuring MAC Table Manipulation

-
-
-
-

Port Security

Command	Purpose
<pre>Router(config)# mac-address-table secure [<mac-address> maximum maximum addresses] fastethernet interface-id [vlan <vlan id>]</pre>	<pre><mac-address> maximum</pre>

Configuring Cisco Discovery Protocol

-
-
-

Configuring the Switched Port Analyzer

Configuring IP Multicast Layer 3 Switching

-
-
-
-

Configuring IGMP Snooping

-
-
- Statically configuring an interface to join a group
- Configuring a multicast router port

IGMP Version 3

In support of the IGMPv3 feature in Cisco IOS Release 12.4(15)T, the **groups** and **count** keywords were added to the **show ip igmp snooping** command, and the output of the **show ip igmp snooping** command was modified to include global information about IGMP snooping groups. Use the **show ip igmp snooping** command with the **groups** keyword to display the multicast table learned by IGMP snooping for all VLANs, or that the **show ip igmp snooping** command with the **groups** keyword, **vlan-id** keyword, and _____ argument to display the multicast table learned by IGMP snooping for a specific VLAN. Use the **show ip igmp snooping** command with the **groups** and **count** keywords to display the number of multicast groups learned by IGMP snooping.

Configuring Per-Port Storm Control

For information on how to configure per-port storm control, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049009

The URL contains information on the following topics:

- Enabling per-port storm-control
- Disabling per-port storm-control

Configuring Fallback Bridging

For information on how to configure fallback bridging, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049176

The URL contains information on the following topics:

- Understanding the default fallback bridging configuration
- Creating a bridge group
- Preventing the forwarding of dynamically learned stations
- Configuring the bridge table aging time
- Filtering frames by a specific MAC address
- Adjusting spanning-tree parameters
- Monitoring and maintaining the network

Configuring Separate Voice and Data Subnets

For information on how to configure separate voice and data subnets, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049866

Managing the Switch

For information on management of the switch, see the following URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049978

The URL contains information on the following topics:

- Adding Trap Managers
- Configuring IP Information
- Enabling Switch Port Analyzer
- Managing the ARP Table
- Managing the MAC Address Tables
- Removing Dynamic Addresses
- Adding Secure Addresses
- Configuring Static Addresses
- Clearing all MAC Address Tables