Configuring Ethernet Switch Ports

This chapter contains the following sections:

- Configuring VLANs, on page 1
- Configuring VTP, on page 2
- Configuring 802.1x Authentication, on page 3
- Configuring Spanning Tree Protocol, on page 4
- Configuring MAC Address Table Manipulation, on page 6
- Configuring Switch Port Analyzer, on page 7
- Configuring Flex Support on Layer 2 and Layer 3 Ports, on page 7
- Configuring IGMP Snooping, on page 10
- Configuring LACP, on page 11
- Configuring HSRP , on page 18
- Configuring VRRP , on page 19

Configuring VLANs

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router. A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment. Any switch port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in the VLAN. Each VLAN is considered a logical network, and packets destined for stations that do not belong to the VLAN must be forwarded through a router.

Note From Cisco IOS XE Release 17.1 through 17.10, the internal VLAN IDs from 2350 – 2449 are configurable.

From Cisco IOS XE Release 17.11.1a, the internal VLAN IDs from 2350 to 2449 are configurable, except those dynamically allocated after the port is switched to L3.

Example: VLAN configuration

```
Router# configure terminal
 Router(config)# vlan 1
 Router(config)# vlan 2
 Router(config)# interface vlan 1
 Router(config-if)# ip address 192.0.2.1 255.255.255.0
 Router(config-if)# no shut
 Router(config-if)# interface vlan 2
 Router(config-if)# ip address 192.0.2.1 255.255.255.0
 Router(config-if)# no shut
 Router(config-if)# interface gigabitethernet 0/1/0
 Router(config-if)# switchport mode access
 Router(config-if)# switchport access vlan 1
 Router(config-if)# interface gigabitethernet 0/1/1
 Router(config-if)# switchport access vlan 2
 Router(config-if)# exit
```

Configuring VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

You should understand the following concepts for configuring VTP.

- VTP domain: A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches or switch stacks under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

- VTP server: In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP Version 3 should be configured on each switch manually including the VTP server and client. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links.VTP server is the default mode.

- VTP client: A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode.

- VTP transparent: VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode.

- VTP pruning is not supported.

For detailed information on VTP, see the following web link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1046901

Example: Configuring VTP

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

```
Router# configure terminal
Router(config)# vtp mode server
Router(config)# vtp domain Lab_Network
Router(config)# exit
```

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

```
Router# configure terminal
Router(config)# vtp domain Lab_Network
Router(config)# vtp mode client
Router(config)# exit
```

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

```
Router# configure terminal
Router(config)# vtp mode transparent
Router(config)# exit
```

Configuring 802.1x Authentication

IEEE 802.1x port-based authentication defines a client-server-based access control and authentication protocol to prevent unauthorized clients from connecting to a LAN through publicly accessible ports.The authentication server authenticates each client connected to a switch port before allowing access to any switch or LAN services. Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic passes through the port.

With IEEE 802.1x authentication, the devices in the network have specific roles:

- Supplicant—Device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The supplicant is sometimes called the client.)

- Authentication server—Device that performs the actual authentication of the supplicant. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services. The Network Access Device transparently passes the authentication messages between the supplicant and the authentication server, and the authentication process is carried out between the supplicant and the authentication server. The particular EAP method used will be decided between the supplicant and the authentication server (RADIUS server). The RADIUS security system with EAP extensions is available in Cisco Secure Access Control Server Version 3.0 or later. RADIUS operates in a client and server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- Authenticator—Router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

For detailed information on how to configure 802.1x port-based authentication, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-mt/sec-user-8021x-15-mt-book/config-ieee-802x-pba.html

Example: Enabling IEEE 802.1x and AAA on a Switch Port

This example shows how to configure Cisco 1100 series router as 802.1x authenticator:

```
Router> enable
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# switchport mode access
Router(config-if)# access-session port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# access-session closed
Router(config-if)# access-session host-mode single-host
Router(config-if)# end
```

Note Cisco 1000 Series Integrated Services Routers do not support the **authentication timer inactivity** command.

Configuring Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree

- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

For detailed configuration information on STP see the following link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html#pgfId-1079138

Example: Spanning Tree Protocol Configuration

The following example shows configuring spanning-tree port priority of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses the port priority when selecting an interface to put in the forwarding state.

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

The following example shows how to change the spanning-tree port cost of a Gigabit Ethernet interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state.

```
Router#configure terminal
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
```

The following example shows configuring the bridge priority of VLAN 10 to 33792:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 priority 33792
Router(config)# end
```

The following example shows configuring the hello time for VLAN 10 being configured to 7 seconds. The hello time is the interval between the generation of configuration messages by the root switch.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 hello-time 7
Router(config)# end
```

The following example shows configuring forward delay time. The forward delay is the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 forward-time 21
Router(config)# end
```

The following example shows configuring maximum age interval for the spanning tree. The maximum-aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

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

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
```

Configuring MAC Address Table Manipulation

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. The address table includes these types of addresses:

- Dynamic address: a source MAC address that the switch learns and then drops when it is not in use. You can use the aging time setting to define how long the switch retains unseen addresses in the table.
- Static address: a manually entered unicast address that does not age and that is not lost when the switch resets.

The address table lists the destination MAC address, the associated VLAN ID, and port associated with the address and the type (static or dynamic).

See the “Example: MAC Address Table Manipulation” for sample configurations for enabling secure MAC address, creating a statc entry, set the maximum number of secure MAC addresses and set the aging time.

For detailed configuration information on MAC address table manipulation see the following link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

Example: MAC Address Table Manipulation

The following example shows creating a static entry in the MAC address table.

```
Router# configure terminal
Router(config)# mac address-table static 0002.0003.0004 interface GigabitEthernet 0/1/0
vlan 3
Router(config)# end
```

The following example shows setting the aging timer.

```
Router# configure terminal
Router(config)# mac address-table aging-time 300
Router(config)# end
```

Configuring Switch Port Analyzer

Cisco 1100 Series ISRs support local SPAN only, and upto one SPAN session. You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source can be monitored by using SPAN; traffic routed to a source cannot be monitored. For example, if incoming traffic is being monitored, traffic that gets routed from another source cannot be monitored; however, traffic that is received on the source and routed to another can be monitored.

For detailed information on how to configure a switched port analyzer (SPAN) session, see the following web link:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swspan.html

Example: SPAN Configuration

The following example shows how to configure a SPAN session to monitor bidirectional traffic from a Gigabit Ethernet source interface:

```
Router# configure terminal
Router(config)# monitor session 1 source gigabitethernet 0/1/0
Router(config)# end
```

The following example shows how to configure a gigabit ethernet interface as the destination for a SPAN session:

```
Router# configure terminal
Router(config)# monitor session 1 destination gigabitethernet 0/1/0
Router(config)# end
```

The following example shows how to remove gigabit ethernet as a SPAN source for SPAN session 1:

```
Router# configure terminal
Router(config)# no monitor session 1 source gigabitethernet 0/1/0
Router(config)# end
```

Configuring Flex Support on Layer 2 and Layer 3 Ports

From Cisco IOS XE Release 17.11.1a, flex support on Layer 2 and Layer 3 ports is enabled on the last two ports of the front-panel Layer 2 switch ports of Cisco 1000 Series ISRs. This provides additional Layer 3 WAN port flexibility on the device. The flex ports can be configured as either a Layer 2 port or a Layer 3 port based on the requirement.

Restrictions for Flex Support on Layer 2 and Layer 3 Ports

- Flex port support is enabled only on Cisco 1000 Series ISRs that have four or eight front-panel switch ports.
- The last two ports of the front-panel fixed ports are the flex ports.
- The two internal VLANs are dynamically reserved for two Layer 3 ports to isolate the Layer 3 traffic and separate the forwarding database for MAC filtering.
- Flex Layer 2 and Layer 3 interfaces do not have PoE support because PoE is enabled only on the half lower number interfaces.
- Weighted Round Robin (WRR) bandwidth and Quality of Service (QoS) mapping configuration are global.
- 802.3x TX pause is not supported on flex Layer 2 and Layer 3 ports.
- PLIM QoS is not supported on flex Layer 3 ports.
- All ingress Layer 3 or Switch Virtual Interfaces (SVI) traffic is throttled if flow control is received.

Supported Platforms

From Cisco IOS XE Release 17.11.1a, the flex support on Layer 2 and Layer 3 ports is available on the Cisco 1000 Series Integrated Services Routers platform.

How to configure Flex Ports

The flex ports are set to Layer 2 interface by default. They can be configured to the Layer 3 port using **no switchport** command and can be returned to the Layer 2 port using **switchport** command. After the interface is converted to Layer 2 or Layer 3, the corresponding Layer 2 or Layer 3 CLIs will be available on that interface.

Configuring Flex Port to Layer 3 Port

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Enters configuration mode for the specified interface on the device.

	Command or Action	Purpose
	`Device(config-if)# interface GigabitEthernet 0/1/6`	
Step 4	**no switchport** **Example:** `Device(config-if)# no switchport`	Converts the port from Layer 2 interface to Layer 3 interface and makes it a routing interface rather than a switch port.
Step 5	**ip address** *address mask* **Example:** `Device(config-if)# ip address 10.10.0.1 255.255.255.0`	Sets the IP address and subnet mask for the specified interface.
Step 6	**exit** **Example:** `Device(config-if)# exit`	Exits configuration mode for the specified interface and returns to global configuration mode.

Configuring Flex Port to Layer 2 Port

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config-if)# interface GigabitEthernet 0/1/6`	Enters configuration mode for the specified interface on the device.
Step 4	**switchport** **Example:** `Device(config-if)# switchport`	Converts the port from Layer 3 interface to Layer 2 interface and makes it a routing interface rather than a switch port.
Step 5	**switchport mode** {**access** | **dynamic** | **trunk trunk** **Example:** `Device(config-if)# switchport mode access`	Configures the operational mode on a Layer 2 interface.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-if)# exit`	Exits configuration mode for the specified interface and returns to global configuration mode.

Configuration Examples

The following are examples of Layer 2 and Layer 3 port configurations.

Example: Flex Port to Layer 3 Port Configuration

The following example shows how to convert a flex port to a Layer 3 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# no switchport
Device(config-if)# ip address 10.10.0.1 255.255.255.0
Device(config-if)# exit
```

Example: Flex Port to Layer 2 Port Configuration

The following example shows how to convert a flex port to a Layer 2 port:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/6
Device(config-if)# switchport
Device(config-if)# switchport mode access
Device(config-if)# exit
```

Verifying Flex Port Configuration

Use the **show platform hardware subslot** *slot*/*card* **module interface** *type number* **status** command to display information about the platform hardware. If the flex port is configured as Layer 3 port, the output displays the L3_NETWORK. If the flex port is configured as Layer 2 port, the output displays the L2_NETWORK.

The following is a sample Layer 3 port configuration verification output:

```
GE6:
MAC Status: hw_port 7, speed 1000, duplex full, link Up, link_en Enable , fc Enable
L3_NETWORK
```

Configuring IGMP Snooping

IGMP snooping constrains the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry.

Use the **`[no] ip igmp snooping enable`** command to configure IGMP Snooping on Cisco 1100 Series ISRs.

By default, IGMP snooping is globally enabled in Cisco 1100 Series ISRs.

Configuring LACP

EtherChannel Overview

EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use the EtherChannel to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

An EtherChannel consists of individual Ethernet links bundled into a single logical link.

The EtherChannel provides full-duplex bandwidth up to 4 Gb/s (Gigabit EtherChannel) between your switch and another switch or host.

Each EtherChannel can consist of up to four compatibly configured Ethernet ports.

Note Port Channel on switchport described in this section is only supported on the C1131 series with enhanced built-in switching hardware and capabilities. It is not supported on other Cisco 1000 Series Integrated Services Routers. Alternatively, you can check L3 port channel on L3 physical interface.

From Cisco IOS XE Dublin 17.11.x release, up to 2 switchports can be configured on the L3 interface for the entire Cisco 1000 Series Integrated Services Routers. For more information, see Configuring LACP (802.3ad) for Gigabit Interfaces.

Channel Groups and Port-Channel Interfaces

An EtherChannel comprises a channel group and a port-channel interface. The channel group binds physical ports to the portchannel interface. Configuration changes applied to the port-channel interface apply to all the physical ports bound together in the channel group. The channel-group command binds the physical port and the port-channel interface together. Each EtherChannel has a port-channel logical interface numbered from 1 to 4 for C1100TG and 1 to 2 for C1131. This port-channel interface number corresponds to the one specified with the channel-group interface configuration command.

Link Aggregation Control Protocol

The LACP is defined in IEEE 802.3ad and enables Cisco devices to manage Ethernet channels between devices that conform to the IEEE 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

By using LACP, the switch learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly, configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single device port.

Auto-LAG

globally and is enabled on all port interfaces. The auto-LAG applies to a switch only when it is enabled globally.

On enabling auto-LAG globally, the following scenarios are possible:

- All port interfaces participate in creation of auto EtherChannels provided the partner port interfaces have EtherChannel configured on them. For more information, see the "The supported auto-LAG configurations between the actor and partner devices" table below.
- Ports that are already part of manual EtherChannels cannot participate in creation of auto EtherChannels.
- When auto-LAG is disabled on a port interface that is already a part of an auto created EtherChannel, the port interface will unbundle from the auto EtherChannel.
- The following table shows the supported auto-LAG configurations between the actor and partner devices:

Table 1: The supported auto-LAG configurations between the actor and partner devices

Actor/Partner	Active	Passive	Auto
Active	Yes	Yes	Yes
Passive	Yes	No	Yes
Auto	Yes	Yes	Yes

On disabling auto-LAG globally, all auto created Etherchannels become manual EtherChannels.

You cannot add any configurations in an existing auto created EtherChannel. To add, you should first convert it into a manual EtherChannel by executing the **port-channel** <*channel-number*> **persistent**.

Configuring Layer 2 EtherChannels

Configure Layer 2 EtherChannels by assigning ports to a channel group with the channel-group command in interface configuration mode. This command automatically creates the port-channel logical interface.

Use the **show etherchannel swport xxx** command to view the C1100TG and C1131 EtherChannels.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**interface***interface-id*
	Example:
	For C1100TG
	`Device(config)# interface gigabitethernet0/2/x`
	Example:
	For C1131
	`Device(config)# interface gigabitethernet0/1/x`
		Specifies a physical port and enters interface configuration mode.
		Valid interfaces are physical ports.
		For a LACP EtherChannel, you can configure up to 4 Ethernet active ports and 4 standby ports (for both C1100TG and C1131) of the same type. Up to 4 ports can be active, and up to 4 ports can be in standby mode.

Step 4	**switchport mode**{**access** | **trunk**}
	Example:
	`Device(config-if)# switchport mode access`
		Assigns all ports as static-access ports in the same VLAN, or configure them as trunks.
		If you configure the port as a static-access port,assign it to only one VLAN. The range is 1 to 4094.

Step 5	**switchport access vlan** *vlan-id* **Example:** `Device(config-if)# switchport access vlan 22`	(Optional) If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.

Step 6	**channel-group** *channel-group-number* **mode** {**on**} | {**active** | **passive**}
	Example:
	`Device(config-if)# channel-group 5 mode passive`
		Assigns the port to a channel group and specifies the LACP mode.
		For mode, select one of these keywords:
		• **on** —Forces the port to channel without LACP. In the on mode, an EtherChannel exists only when a port-group in the on mode is connected to another port group in the on mode.
		• **active**—Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
		• **• passive** —Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives but does not start LACP packet negotiation.

	Command or Action	Purpose

Step 7	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

In the above table, the port-channel interface is created implicitly through the "channel-group" command. An alternate way is to create the port-channel interface explicitly with the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** **Example:** `Device(config)#interface portchannel [interface-number]`	Creates the port-channel interface that by default, creates the Layer 3 interface.
Step 4	**switchport interface** **Example:** `Device(config-if)#switchport`	Assigns switch port-channel interface to layer 2 switching interface.

Step 5	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring EtherChannel Load-Balancing

You can configure EtherChannel load-balancing to use one of several different forwarding methods. This task is optional.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 2	**port-channel swport load-balance** {**dst-ip** | **dst-mac** | **dst-mixed-ip-port** | **dst-port** | **src-dst-ip** | **src-dst-mac** | **src-dst-mixed-ip-port** | **src-dst-port** | **src-ip** | **src-mac** | **src-mixed-ip-port** | **src-port**}
	Example:
	For C1100TG
	`Device(config)# port-channel swport load-balance src-mac`
		Select one of these load-distribution methods:
		a. dst-ip—Specifies destination-host IP address.
		b. dst-mac—Specifies the destination-host MAC address of the incoming packet.
		c. dst-mixed-ip-port—Specifies the host IP address and TCP/UDP port.
		d. dst-port—Specifies the destination TCP/UDP port.
		e. src-dst-ip—Specifies the source and destination host IP address.
		f. src-dst-mac—Specifies the source and destination host MAC address.
		g. src-dst-mixed-ip-port—Specifies the source and destination host IP address and TCP/UDP port.
		h. src-dst-port—Specifies the source and destination TCP/UDP port.
		i. src-ip—Specifies the source host IP address.
		j. src-mac—Specifies the source MAC address of the incoming packet.
		k. src-mixed-ip-port—Specifies the source host IP address and TCP/UDP port.
		l. src-port—Specifies the source TCP/UDP port.

Step 3	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring the LACP Port Channel Min-Links Feature

You can specify the minimum number of active ports that must be in the link-up state and bundled in an EtherChannel for the port channel interface to transition to the link-up state. Using EtherChannel min-links, you can prevent low-bandwidth LACP EtherChannels from becoming active. Port channel min-links also cause LACP EtherChannels to become inactive if they have too few active member ports to supply the required minimum bandwidth.

To configure the minimum number of links that are required for a port channel. Perform the following tasks.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** `Device(config)# interface port-channel 2`	Enters interface configuration mode for a port-channel. For channel-number, the range is 1 to 4 for C1100TG and 1 to 2 for C1131.
Step 4	**port-channel min-links***min-links-number* **Example:** `Device(config-if)# port-channel min-links 3`	Specifies the minimum number of member ports that must be in the link-up state and bundled in the EtherChannel for the port channel interface to transition to the link-up state. For min-links-number, the range is 1 to 4 for C1100TG and 1 to 2 for C1131.

Step 5	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring LACP Fast Rate Timer

You can change the LACP timer rate to modify the duration of the LACP timeout. Use the lacp rate command to set the rate at which LACP control packets are received by an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose

Step 3	**interface** {**gigabitethernet**}*slot/subslot/port*
	Example:
	For C1100TG
	`Device(config)# interface gigabitEthernet 0/2/x`
	Example:
	For C1131
	`Device(config)# interface gigabitEthernet 0/1/x`
		Configures an interface and enters interface configuration mode.

Step 4	**lacp rate**{**normal** | **fast**}
	Example:
	`Device(config-if)# lacp rate fast`
		Configures the rate at which LACP control packets are received by an LACP-supported interface. To reset the timeout rate to its default, use the **no lacp rate** command.

Step 5	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Step 6	**show lacp internal**
	Example:
	`Device# show lacp internal`
	`Device# show lacp counters`
		Verifies your configuration.

Configuring Auto-LAG Globally

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	[**no**]**port-channel swportauto** **Example:** `Device(config)# port-channel swport auto`	Enables the auto-LAG feature on a switch globally. Use the no form of this command to disable the auto-LAG feature on the switch globally. **Note** By default, the auto-LAG feature is enabled on the port

	Command or Action	Purpose

Step 4	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Step 5	**show etherchannel swport auto** **Example:** `Device# show etherchannel swport auto`	Displays that EtherChannel is created automatically.

Configuring HSRP

Note HSRP is supported only on the SVI interface.

The Hot Standby Router Protocol (HSRP) is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

HSRP uses a priority mechanism to determine which HSRP configured device is to be the default active device. To configure a device as the active device, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure just one device to have a higher priority, that device will be the default active device. In case of ties, the primary IP addresses are compared, and the higher IP address has priority. If you do not use the standby preempt interface configuration command in the configuration for a router, that router will not become the active router, even if its priority is higher than all other routers.

For more information about configuring HSRP, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-hsrp.html

Example: Configuring HSRP

In this example, Router A is configured to be the active device for group 1 and standby device for group 2. Device B is configured as the active device for group 2 and standby device for group 1.

```
RouterA# configure terminal
RouterA(config)# interface vlan 2
RouterA(config-if)# ip address 10.1.0.21 255.255.0.0
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.0.3
RouterA(config-if)# standby 2 priority 95
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 ip 10.1.0.4
RouterA(config-if)# end

RouterB# configure terminal
RouterB(config)# interface vlan 2
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.0.3
RouterB(config-if)# standby 2 priority 110
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.1.0.4
```

Configuring VRRP

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the primary virtual router, with the other routers acting as backups in case the primary virtual router fails.

An important aspect of the VRRP is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the primary virtual router fails. If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a primary virtual router. Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming a primary virtual router if the primary virtual router fails. You can configure the priority of each virtual router backup using the vrrp priority command.

By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become primary virtual router. You can disable this preemptive scheme using the no vrrp preempt command. If preemption is disabled, the virtual router backup that is elected to become virtual router primary remains the primary until the original primary virtual router recovers and becomes primary again.

The primary virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the primary virtual router. The VRRP advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

For more information on VRRP, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html

Example: Configuring VRRP

In the following example, Router A and Router B each belong to two VRRP groups, group1 and group 5. In this configuration, each group has the following properties:

Group 1:

- Virtual IP address is 10.1.0.10.
- Router A will become the primary for this group with priority 120.
- Advertising interval is 3 seconds.
- Preemption is enabled.

Group 5:

- Router B will become the primary for this group with priority 200.
- Advertising interval is 30 seconds.
- Preemption is enabled.

```
RouterA(config)# interface vlan 2
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip 10.1.0.10
RouterA(config-if)# vrrp 5 priority 100
RouterA(config-if)# vrrp 5 timers advertise 30
RouterA(config-if)# vrrp 5 timers learn
RouterA(config-if)# vrrp 5 ip 10.1.0.50
RouterA(config-if)# no shutdown
RouterA(config-if)# end
RouterB(config)# interface vlan 2
RouterB(config-if)# ip address 10.1.0.1 255.0.0.0
RouterB(config-if)# vrrp 1 priority 100
RouterB(config-if)# vrrp 1 authentication cisco
RouterB(config-if)# vrrp 1 timers advertise 3
RouterB(config-if)# vrrp 1 timers learn
RouterB(config-if)# vrrp 1 ip 10.1.0.10
RouterB(config-if)# vrrp 5 priority 200
RouterB(config-if)# vrrp 5 timers advertise 30
RouterB(config-if)# vrrp 5 timers learn
RouterB(config-if)# vrrp 5 ip 10.1.0.50
RouterB(config-if)# no shutdown
RouterB(config-if)# end
```