High Availability and Redundancy Software Configuration Guide for Cisco IE 2000U and Connected Grid Switches

First Published: July 2013
Last Updated: July 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

CHAPTER 1

Overview

This chapter provides an overview of the high availability and redundancy features supported on the Cisco Industrial Ethernet 2000U Series (IE2000) and Connected Grid Switches, hereafter referred to as switch. This chapter includes the following sections:

- Flex Links, page 1-1
- MAC Address Table Move Update, page 1-2
- EtherChannels, page 1-2
- Link-state Tracking, page 1-2
- Hot Standby Router Protocol (HSRP), page 1-2

Flex Links

Flex Links are a pair of a Layer 2 interfaces (switchports or port channels), where one interface is configured to act as a backup to the other.

Flex Links provide an alternative solution to the Spanning Tree Protocol (STP), allowing users to turn off STP and still provide basic link redundancy. Generally, you configure Flex Links in networks where customers do not want to run STP on the switch. When the switch is running STP, it is not necessary to configure Flex Links because STP already provides link-level redundancy or backup.

Related Topics

Chapter 2, “Configuring Flex Links and MAC Address-Table Move Update”

MAC Address Table Move Update

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence when a primary (forwarding) link goes down and the standby link begins forwarding traffic.

Related Topics

Chapter 2, "Configuring Flex Links and MAC Address-Table Move Update"

EtherChannels

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

Etherchannels provide fault-tolerant high-speed links between switches, routers, and servers.

You can use an EtherChannel to increase the bandwidth between points within the network; and, to address bottlenecks within the network.

EtherChannels provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, then the EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

Related Topics

Chapter 3, "Configuring EtherChannels and Link-State Tracking"

Link-state Tracking

Link-state tracking, also known as trunk failover, binds the link state of multiple interfaces. Link-state tracking provides redundancy in the network when used with Flex Links. If the link is lost on the primary interface, the router transparently switches the connectivity to the secondary interface.

Related Topics

Chapter 3, "Configuring EtherChannels and Link-State Tracking"

Chapter 2, "Configuring Flex Links and MAC Address-Table Move Update"

Hot Standby Router Protocol (HSRP)

HSRP is a 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 you configure HSRP on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that a group of configured routers share.

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; rather, 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.

Related Topics

Chapter 4, "Configuring HSRP"

CHAPTER 2

Configuring Flex Links and MAC Address-Table Move Update

This chapter describes how to configure Flex Links and MAC address-table move update, also known as Flex Links bidirectional fast convergence, on the Cisco Industrial Ethernet 2000U Series (IE2000 U) and Connected Grid Switches, hereafter referred to as switch. Flex Links are a pair of interfaces that provide a mutual backup.

The chapter includes the following sections:

Information About Flex Links and MAC Address-Table Move Update

This section includes the following topics:

Flex Links

Flex Links are a pair of a Layer 2 interfaces (switchports or port channels), where one interface is configured to act as a backup to the other.

This feature provides an alternative solution to the Spanning Tree Protocol (STP), allowing users to turn off STP and still provide basic link redundancy. You generally configure Flex Links in networks where customers do not want to run STP on the switch. When you configure STP on the switch, it is not necessary to configure Flex Links because STP already provides link-level redundancy or backup.

Note STP is enabled by default on network node interfaces (NNIs). It is disabled on enhanced network interfaces (ENIs), but you can enable it. STP is not supported on user network interfaces (UNIs).

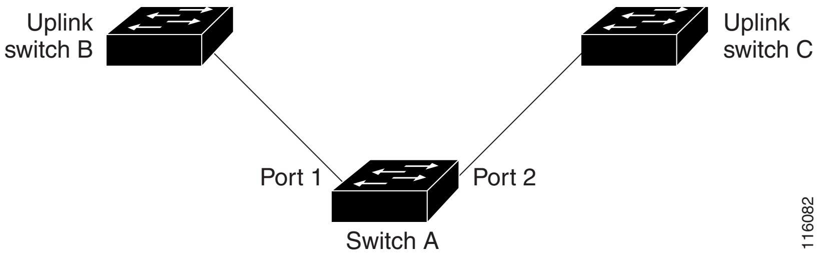
You configure Flex Links on one Layer 2 interface (the active link) by assigning another Layer 2 interface as the Flex Link or backup link. When one of the links is up and forwarding traffic, the other link is in standby mode, ready to begin forwarding traffic if the other link shuts down. At any given time, only one of the interfaces is in the linkup state and forwarding traffic. If the primary link shuts down, the standby link starts forwarding traffic. When the active link comes back up, it goes into standby mode and does not forward traffic. STP is disabled on Flex Link interfaces.

In Figure 2-1, ports 1 and 2 on switch A are connected to uplink switches B and C. Because they are configured as Flex Links, only one of the interfaces is forwarding traffic; the other is in standby mode. If port 1 is the active link, it begins forwarding traffic between port 1 and switch B; the link between port 2 (the backup link) and switch C is not forwarding traffic. If port 1 goes down, port 2 comes up and starts forwarding traffic to switch C. When port 1 comes back up, it goes into standby mode and does not forward traffic; port 2 continues forwarding traffic.

Preemption

You can also choose to configure a preemption mechanism, specifying the preferred port for forwarding traffic. In Figure 2-1, for example, you can configure the Flex Link pair with preemption mode so that after port 1 comes back up in the scenario, if it has greater bandwidth than port 2, port 1 begins forwarding after 60 seconds; and port 2 becomes the standby. You do this by entering the interface configuration **switchport backup interface preemption mode bandwidth** and **switchport backup interface preemption delay** commands.

Figure 2-1 Flex Links Configuration Example



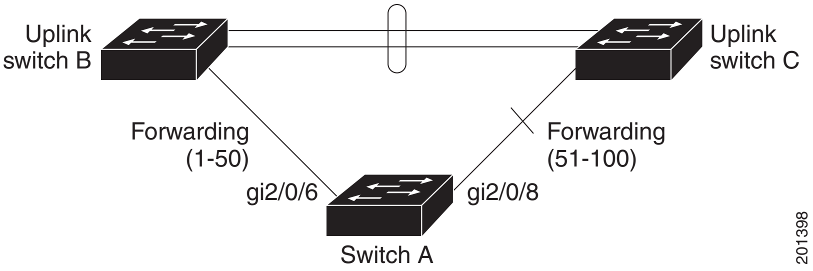
If a primary (forwarding) link goes down, a trap notifies the network management stations. If the standby link goes down, a trap notifies the users.

Flex Links are supported only on Layer 2 ports and port channels, not on VLANs or Layer 3 ports.

VLAN Flex Link Load Balancing and Support

VLAN Flex Link load-balancing allows users to configure a Flex Link pair so that both ports simultaneously forward the traffic for some mutually exclusive VLANs. For example, if Flex Link ports are configured for 1-100 VLANs, the traffic of the first 50 VLANs can be forwarded on one port and the rest on the other port. If one of the ports fail, the other active port forwards all the traffic. When the failed port comes back up, it resumes forwarding traffic in the preferred vlans. This way, apart from providing the redundancy, this Flex Link pair can be used for load balancing. Also, Flex Link VLAN load-balancing does not impose any restrictions on uplink switches.

Figure 2-2 VLAN Flex Links Load Balancing Configuration Example



Flex Link Multicast Fast Convergence

Flex Link Multicast Fast Convergence reduces the multicast traffic convergence time after a Flex Link failure. This is implemented by a combination of these solutions:

- Learning the Other Flex Link Port as the mrouter Port, page 2-3
- Generating IGMP Reports, page 2-4
- Leaking IGMP Reports, page 2-4

Learning the Other Flex Link Port as the mrouter Port

In a typical multicast network, there is a querier for each VLAN. A switch deployed at the edge of a network has one of its Flex Link ports receiving queries. Flex Link ports are also always forwarding at any given time.

A port that receives queries is added as an *mrouter* port on the switch. An mrouter port is part of all the multicast groups learned by the switch. After a changeover, queries are received by the other Flex Link port. The other Flex Link port is then learned as the mrouter port. After changeover, multicast traffic then flows through the other Flex Link port. To achieve faster convergence of traffic, both Flex Link ports are learned as mrouter ports whenever either Flex Link port is learned as the mrouter port. Both Flex Link ports are always part of multicast groups.

Though both Flex Link ports are part of the groups in normal operation mode, all traffic on the backup port is blocked. So the normal multicast data flow is not affected by the addition of the backup port as an mrouter port. When the changeover happens, the backup port is unblocked, allowing the traffic to flow. In this case, the upstream multicast data flows as soon as the backup port is unblocked.

Generating IGMP Reports

When the backup link comes up after the changeover, the upstream new distribution switch does not start forwarding multicast data, because the port on the upstream router, which is connected to the blocked Flex Link port, is not part of any multicast group. The reports for the multicast groups were not forwarded by the downstream switch because the backup link is blocked. The data does not flow on this port, until it learns the multicast groups, which occurs only after it receives reports.

The reports are sent by hosts when a general query is received, and a general query is sent within 60 seconds in normal scenarios. When the backup link starts forwarding, to achieve faster convergence of multicast data, the downstream switch immediately sends proxy reports for all the learned groups on this port without waiting for a general query.

Leaking IGMP Reports

To achieve multicast traffic convergence with minimal loss, a redundant data path must be set up before the Flex Link active link goes down. This can be achieved by leaking only IGMP report packets on the Flex Link backup link. These leaked IGMP report messages are processed by upstream distribution routers, so multicast data traffic gets forwarded to the backup interface. Because all incoming traffic on the backup interface is dropped at the ingress of the access switch, no duplicate multicast traffic is received by the host. When the Flex Link active link fails, the access switch starts accepting traffic from the backup link immediately. The only disadvantage of this scheme is that it consumes bandwidth on the link between the distribution switches and on the backup link between the distribution and access switches. This feature is disabled by default and can be configured by using the **switchport backup interface** *interface-id* **multicast fast-convergence** command.

When this feature has been enabled at changeover, the switch does not generate the proxy reports on the backup port, which became the forwarding port.

Configuration Examples

This configuration example shows learning the other Flex Link port as the mrouter port when Flex Link is configured on Gigabit Ethernet interface 0/11 and Gigabit Ethernet interface 0/12. The example shows the output for the **show interfaces switchport backup** command:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport backup interface Gi0/12
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/12
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface Backup Interface State
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : Off
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLANs 1 and 401, with their queries reaching the switch through Gigabit Ethernet interface 0/11:

```
Switch# show ip igmp snooping querier
```

```
Vlan    IP Address     IGMP Version       Port
-------------------------------------------------------------
1       1.1.1.1        v2                 Gi0/11
401     41.41.41.1     v2                 Gi0/11
```

This is output for the **show ip igmp snooping mrouter** command for VLANs 1 and 401:

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
1       Gi1/0/11(dynamic), Gi0/12(dynamic)
401     Gi1/0/11(dynamic), Gi0/12(dynamic)
```

Similarly, both Flex Link ports are part of learned groups. In this example, Gigabit Ethernet interface 0/10 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups
Vlan    Group      Type    Version     Port List
-----------------------------------------------------------------------
1       228.1.5.1  igmp    v2          Gi0/11, Gi0/12, Gi0/10
1       228.1.5.2  igmp    v2          Gi0/11, Gi0/12, Gi0/10
```

When a host responds to the general query, the switch forwards this report on all the mrouter ports. In this example, when a host sends a report for the group 228.1.5.1, it is forwarded only on Gigabit Ethernet interface 0/11, because the backup port Gigabit Ethernet 0/12 interface is blocked. When the active link, Gigabit Ethernet interface 0/11, goes down, the backup port, Gigabit Ethernet interface 0/12, begins forwarding.

As soon as this port starts forwarding, the switch sends proxy reports for the groups 228.1.5.1 and 228.1.5.2 on behalf of the host. The upstream router learns the groups and starts forwarding multicast data. This is the default behavior of Flex Link. This behavior changes when the user configures fast convergence using the **switchport backup interface gigabitethernet 0/12 multicast fast-convergence** command. This example shows turning on this feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitEthernet0/11
Switch(config-if)# switchport backup interface gigabitEthernet0/12 multicast
fast-convergence
Switch(config-if)# exit
Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active                 Interface             Backup Interface State
------------------------------------------------------------------------
GigabitEthernet0/11 GigabitEthernet0/12 Active Up/Backup Standby
Preemption Mode : off
Multicast Fast Convergence : On
Bandwidth : 100000 Kbit (Gi0/11), 100000 Kbit (Gi0/12)
Mac Address Move Update Vlan : auto
```

This output shows a querier for VLAN 1 and 401 with their queries reaching the switch through Gigabit Ethernet interface 0/11:

```
Switch# show ip igmp snooping querier
Vlan        IP Address     IGMP Version   Port
-------------------------------------------------------------
1           1.1.1.1        v2             Gi0/11
401         41.41.41.1     v2             Gi0/11
```

This is output for the **show ip igmp snooping mrouter** command for VLAN 1 and 401:

```
Switch# show ip igmp snooping mrouter
Vlan        ports
```

```
----        -----
1           Gi0/11(dynamic), Gi0/12(dynamic)
401         Gi0/11(dynamic), Gi0/12(dynamic)
```

Similarly, both the Flex Link ports are a part of the learned groups. In this example, Gigabit Ethernet interface 0/10 is a receiver/host in VLAN 1, which is interested in two multicast groups:

```
Switch# show ip igmp snooping groups
Vlan    Group       Type    Version     Port List
-----------------------------------------------------------------------
1       228.1.5.1   igmp    v2          Gi0/11, Gi0/12, Gi0/10
1       228.1.5.2   igmp    v2          Gi1/0/11, Gi0/12, Gi0/10
```

When a host responds to the general query, the switch forwards this report on all the mrouter ports. When you turn on this feature through the command-line port, and when a report is forwarded by the switch on Gigabit Ethernet interface 0/11, it is also leaked to the backup port Gigabit Ethernet interface 0/12. The upstream router learns the groups and starts forwarding multicast data, which is dropped at the ingress because Gigabit Ethernet interface 0/12 is blocked. When the active link, Gigabit Ethernet interface 0/11, goes down, the backup port, Gigabit Ethernet interface 0/12, begins forwarding. You do not need to send any proxy reports as the multicast data is already being forwarded by the upstream router. By leaking reports to the backup port, a redundant multicast path has been set up, and the time taken for the multicast traffic convergence is very minimal.

MAC Address-Table Move Update

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence when a primary (forwarding) link goes down and the standby link begins forwarding traffic.

In Figure 2-3, switch A is an access switch, and ports 1 and 2 on switch A are connected to uplink switches B and D through a Flex Link pair. Port 1 is forwarding traffic, and port 2 is in the backup state. Traffic from the PC to the server is forwarded from port 1 to port 3. The MAC address of the PC has been learned on port 3 of switch C. Traffic from the server to the PC is forwarded from port 3 to port 1.

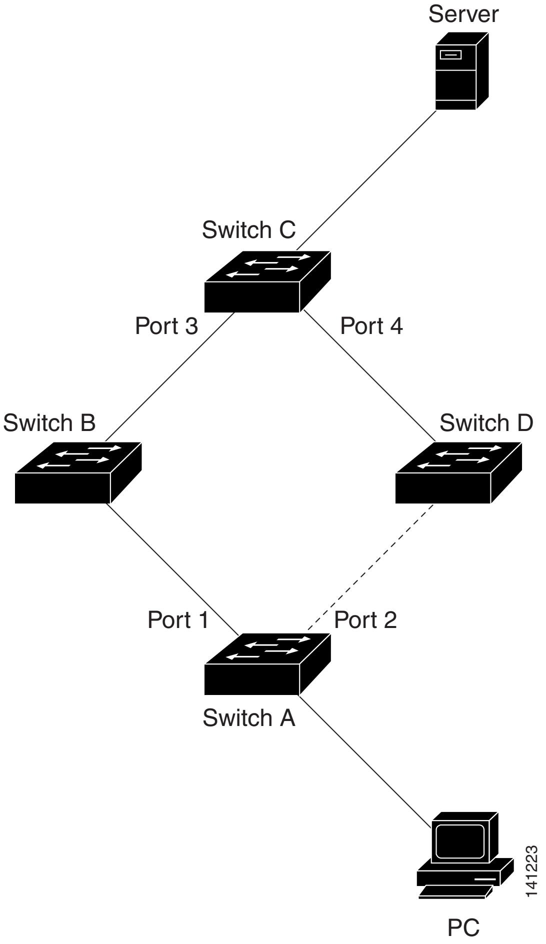
If the MAC address-table move update feature is not configured and port 1 goes down, port 2 starts forwarding traffic. However, for a short time, switch C keeps forwarding traffic from the server to the PC through port 3, and the PC does not get the traffic because port 1 is down. If switch C removes the MAC address of the PC on port 3 and relearns it on port 4, traffic can then be forwarded from the server to the PC through port 2.

If the MAC address-table move update feature is configured and enabled on the switches in Figure 2-3 and port 1 goes down, port 2 starts forwarding traffic from the PC to the server. The switch sends a MAC address-table move update packet from port 2. Switch C gets this packet on port 4 and immediately learns the MAC address of the PC on port 4, which reduces the reconvergence time.

You can configure the access switch, switch A, to *send* MAC address-table move update messages. You can also configure the uplink switches B, C, and D to *get* and process the MAC address-table move update messages. When switch C gets a MAC address-table move update message from switch A, switch C learns the MAC address of the PC on port 4. Switch C updates the MAC address table, including the forwarding table entry for the PC.

Switch A does not need to wait for the MAC address-table update. The switch detects a failure on port 1 and immediately starts forwarding server traffic from port 2, the new forwarding port. This change occurs in 100 milliseconds (ms). The PC is directly connected to switch A, and the connection status does not change. Switch A does not need to update the PC entry in the MAC address table.

Figure 2-3 MAC Address-Table Move Update Example



Guidelines and Limitations

Flex Links

- You can configure up to 16 backup Flex Links.
- You can configure only one Flex Link backup link for any active link, and it must be on a different interface than the active interface.
- An interface can belong to only one Flex Link pair.
- An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- Neither of the links (active or backup) can be a port that belongs to an EtherChannel.

  However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.

- A backup link does not have to be the same type (Fast Ethernet, Gigabit Ethernet, or port channel) as the active link. However, we recommend that you configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- STP is disabled on Flex Link ports. When STP is configured on the switch, Flex Links do not participate in STP within any VLANs. Ensure that there are no loops in the configured topology, when not operating with STP.

Note STP is available only on NNIs or ENIs.

Preemption

- You cannot configure a preemption mechanism and VLAN load balancing for the same Flex Links pair.

VLAN Load Balancing on Flex Links

- For Flex Link VLAN load balancing, you must choose the preferred VLANs on the backup interface.
- You cannot configure a preemption mechanism and VLAN load balancing for the same Flex Links pair.

MAC Address Table Move Update

- You can enable and configure this feature on the access switch to *send* the MAC address-table move updates.
- You can enable and configure this feature on the uplink switches to *get* the MAC address-table move updates.

Default Settings

Parameters	Default
Flex links	Disabled
Flex links preemption mode	Off
Flex links preemption delay	35 seconds
Flex link VLAN load-balancing	Disabled
MAC address table move update	Disabled

Configuring Flex Links and MAC Address Table Move Update

- Enabling the Flex Link, page 2-9
- Defining a Flex Link Preemption Scheme, page 2-10
- Configuring VLAN Load Balancing on Flex Links, page 2-11
- Configuring MAC Address-Table Move Update, page 2-12

Enabling the Flex Link

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface, and enters interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and network NNIs are enabled.
Step 4	**switchport backup interface** *interface-id*	Configures the backup link for the interface defined in Step 2. **Note** When one interface is forwarding traffic, the other interface is in standby mode.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure an interface with a backup interface:

```
Switch# configure terminal
Switch(conf)# interface fastethernet0/1
Switch(conf-if)# no shutdown
Switch(conf-if)# switchport backup interface fastethernet0/2
Switch(conf-if)# end

Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 preemption mode forced
Switch(conf-if)# switchport backup interface gigabitethernet0/2 preemption delay 50
```

Defining a Flex Link Preemption Scheme

Configure a preemption scheme for the Flex Links pair (active and backup links).

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

Define and enable the Flex Link. (See Enabling the Flex Link.)

Determine what preemption mode, if any, you want to assign to the port. (See Preemption.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface on which you want to define the preemption scheme.
Step 3	**switchport backup interface** *interface-id* **preemption mode** {**forced** | **bandwidth** | **off**}	Configure a preemption mechanism and delay for a Flex Link pair. You can configure the preemption as: • **forced**—the active interface always preempts the backup. • **bandwidth**—the interface with the higher bandwidth always acts as the active interface. • **off**—no preemption happens from active to backup.
Step 4	**switchport backup interface** *interface-id* **preemption delay** *delay-time*	Configure the time delay until a port preempts another port. **Note** Setting a delay time only works with forced and bandwidth modes.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure the preemption mode as *forced* for a backup interface pair:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 preemption mode forced
Switch(conf-if)# switchport backup interface gigabitethernet0/2 preemption delay 50
Switch(conf-if)# end
```

Configuring VLAN Load Balancing on Flex Links

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

Define and enable the Flex Link. (See Enabling the Flex Link.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport backup interface** *interface-id* **prefer vlan** *vlan-range*	Configure a physical Layer 2 interface (or port channel) as part of a Flex Links pair with the interface, and specify the VLANs carried on the interface. The VLAN ID range is 1 to 4094.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

In the following example, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

When both interfaces are up, Gigabit Ethernet port 0/8 forwards traffic for VLANs 60 and 100 to 120 and Gigabit Ethernet port 0/6 forwards traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gigabit Ethernet port 0/6 goes down, Gigabit Ethernet port 0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
```

```
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface 0/6 comes up, VLANs preferred on this interface are blocked on the peer interface 0/8 and forwarded on 0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Standby

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120

Switch# show interfaces switchport backup detail
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
FastEthernet 0/3       FastEthernet 0/4       Active Down/Backup Up

Vlans Preferred on Active Interface: 1-2,5-4094
Vlans Preferred on Backup Interface: 3-4
Preemption Mode  : off
Bandwidth : 10000 Kbit (Fa 0/3), 100000 Kbit (Fa0/4)
Mac Address Move Update Vlan : auto
```

Configuring MAC Address-Table Move Update

Configuring a switch to send and get MAC address-table move updates.

Sending MAC Address Table Move Updates

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface, and enter interface configuration mode. The interface can be a physical Layer 2 interface or a port channel (logical interface). The port-channel range is 1 to 48.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 4	**switchport backup interface** *interface-id* or **switchport backup interface** *interface-id* **mmu primary vlan** *vlan-id*	Configure a physical Layer 2 interface (or port channel), as part of a Flex Link pair with the interface. The MAC address-table move update VLAN is the lowest VLAN ID on the interface. Configure a physical Layer 2 interface (or port channel) and specify the VLAN ID on the interface, which is used for sending the MAC address-table move update. When one link is forwarding traffic, the other interface is in standby mode.
Step 5	**end**	Return to global configuration mode.
Step 6	**mac address-table move update transmit**	Enable the access switch to send MAC address-table move updates to other switches in the network if the primary link goes down and the switch starts forwarding traffic through the standby link. To disable the MAC address-table move update feature, use the **no mac address-table move update transmit** interface configuration command.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure an access switch to send MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet0/1
Switch(conf-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 2
Switch(conf-if)# exit
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

Getting MAC Address Table Move Updates

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac address-table move update receive**	Enable the switch to get and process the MAC address-table move updates. To disable the MAC address-table move update feature, use the **no mac address-table move update receive** configuration command.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**copy running-config startup config**	(Optional) Save your entries in the switch startup configuration file.

EXAMPLE

This example shows how to configure a switch to get and process MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

Verifying Configuration

Command	Purpose
show interface [*interface-id*] **switchport backup [detail]**	Displays the Flex Link backup interface configured for an interface, or displays all Flex Links configured on the switch and the state of each active and backup interface (up or standby mode).
show mac address-table move update	Displays the MAC address-table move update information on the switch.

EXAMPLE

This example shows summary configuration information for the Flex Link pair.

```
Switch# show interface switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------------------------
FastEthernet0/1         FastEthernet0/2         Active Up/Backup Standby
FastEthernet0/3         FastEthernet0/4         Active Up/Backup Standby
Port-channel1           GigabitEthernet0/1      Active Up/Backup Standby
```

This example shows detailed configuration information for the Flex Link pair.

```
Switch# show interface switchport backup detail
Active Interface Backup Interface State
------------------------------------------------------------------------
GigabitEthernet0/21 GigabitEthernet0/2 Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : forced
Preemption Delay : 50 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
Mac Address Move Update Vlan : auto
```

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

Configuring EtherChannels and Link-State Tracking

This chapter describes how to configure EtherChannel on Layer 2 and Layer 3 ports and Link-state Tracking on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as switch.

This chapter includes the following sections:

- Information About EtherChannels, page 3-1
- Prerequisites, page 3-9
- Default Settings, page 3-12
- Configuring EtherChannels, page 3-12
- Verifying EtherChannel, PAgP, and LACP Configuration, page 3-24
- Information About Link-State Tracking, page 3-25
- Guidelines and Limitations, page 3-25
- Default Settings, page 3-26
- Configuring Link-State Tracking, page 3-26
- Verifying Link-State Tracking Configuration, page 3-27
- Configuration Example, page 3-28
- Feature History, page 3-28

Information About EtherChannels

This section includes the following topics:

- EtherChannel Overview, page 3-2
- Port-Channel Interfaces, page 3-3
- Port Aggregation Protocol, page 3-4
- Link Aggregation Control Protocol, page 3-6
- EtherChannel On Mode, page 3-7
- Load Balancing and Forwarding Methods, page 3-8

EtherChannel Overview

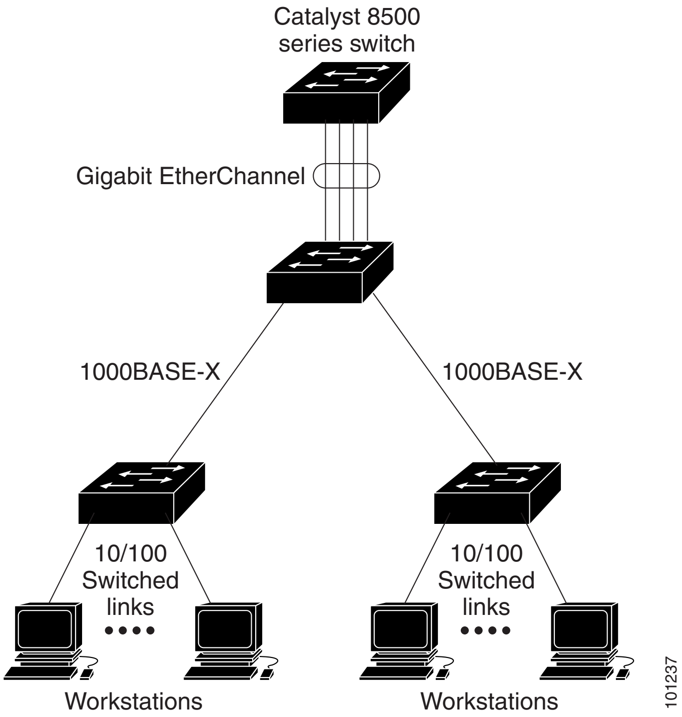
An EtherChannel consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link as shown in Figure 3-1.

Etherchannels provide fault-tolerant high-speed links between switches, routers, and servers.

You can use an EtherChannel to increase the bandwidth between points within the network; and, to address bottlenecks within the network.

EtherChannels provide automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, then the EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

Figure 3-1 Typical EtherChannel Deployment



EtherChannel provides full-duplex bandwidth of up to 800 Mbps between your switch and another switch or host for Fast EtherChannel on a switch with 24 Fast Ethernet ports. For Gigabit EtherChannel, you can configure up to 8 Gbps (8 ports of 1 Gbps), depending on the number of supported Gigabit Ethernet interfaces.

Each EtherChannel can consist of up to eight compatibly configured Ethernet ports. All ports in each EtherChannel must be configured as either Layer 2 or Layer 3 ports. The number of EtherChannels is limited to 48. For more information, see the "Guidelines and Limitations" section on page 3-10. The EtherChannel Layer 3 ports are made up of routed ports. Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.

Operating Modes

You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or **On** mode. PAgP and LACP are available only on NNIs and ENIs. Configure both ends of the EtherChannel in the same mode:

- When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. Incompatible ports are suspended.
- When you configure an EtherChannel in the **on** mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the **On** mode; otherwise, packet loss can occur.

  The local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

If a link within an EtherChannel fails, traffic previously carried over that failed link changes to the remaining links within the EtherChannel. A trap is sent for a failure, identifying the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

Port-Channel Interfaces

When you create an EtherChannel, a port-channel logical interface is involved.

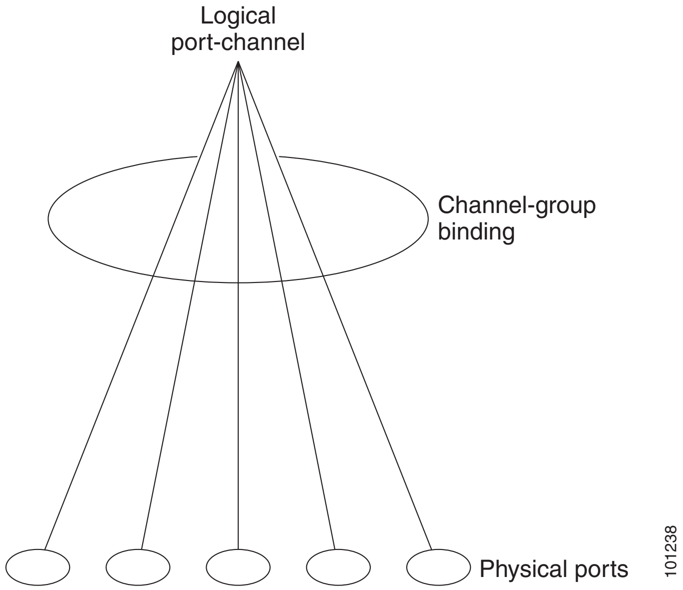
- With Layer 2 ports, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface.

  You also can use the **interface port-channel** *port-channel-number* global configuration command to manually create the port-channel logical interface, but then you must use the **channel-group** *channel-group-number* command to bind the logical interface to a physical port. The *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.
- With Layer 3 ports, you should manually create the logical interface by using the **interface port-channel** global configuration command followed by the **no switchport** interface configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command.

For both Layer 2 and Layer 3 ports, the **channel-group** command binds the physical port and the logical interface together as shown in Figure 3-2.

Each EtherChannel has a port-channel logical interface numbered from 1 to 48. This port-channel interface number corresponds to the one specified with the **channel-group** interface configuration command.

Figure 3-2 Relationship of Physical Ports, Logical Port Channels, and Channel Groups



After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port to which you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port-channel interface.

Port Aggregation Protocol

The Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that can be run only on Cisco switches and on those switches licensed by vendors to support PAgP. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports.

Note PAgP is only available on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

By using PAgP, the switch learns the identity of partners capable of supporting PAgP 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, PAgP 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, PAgP adds the group to the spanning tree as a single switch port.

PAgP Modes

Table 3-1 shows the user-configurable EtherChannel PAgP modes for the **channel-group** interface configuration command on an NNI or ENI.

Table 3-1 EtherChannel PAgP Modes

Mode	Description
auto	Places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.
desirable	Places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets.

Switch ports exchange PAgP packets only with partner ports configured in the **auto** or **desirable** modes. Ports configured in the **on** mode do not exchange PAgP packets.

Both the **auto** and **desirable** modes enable ports to negotiate with partner ports to form an EtherChannel based on criteria such as port speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.

Ports can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:

- A port in the **desirable** mode can form an EtherChannel with another port that is in the **desirable** or **auto** mode.
- A port in the **auto** mode can form an EtherChannel with another port that is in the **desirable** mode.

A port in the **auto** mode cannot form an EtherChannel with another port that is also in the **auto** mode because neither port starts PAgP negotiation.

If your switch is connected to a partner that is PAgP-capable, you can configure the switch port for nonsilent operation by using the **non-silent** keyword. If you do not specify **non-silent** with the **auto** or **desirable** mode, silent mode is assumed.

Use the silent mode when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port connected to a silent partner prevents that switch port from ever becoming operational. However, the silent setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.

PAgP Learn Method and Priority

Configures your switch as a PAgP physical-port learner and adjusts the priority so that the same port in the bundle is selected for sending packets.

Network devices are classified as PAgP physical learners or aggregate-port learners. A device is a physical learner if it learns addresses by physical ports and directs transmissions based on that knowledge. A device is an aggregate-port learner if it learns addresses by aggregate (logical) ports. The learn method must be configured the same at both ends of the link.

Note PAgP is available only on NNIs and ENIs.

When a device and its partner are both aggregate-port learners, they learn the address on the logical port-channel. The device sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives.

PAgP cannot automatically detect when the partner device is a physical learner and when the local device is an aggregate-port learner. Therefore, you must manually set the learning method on the local device to learn addresses by physical ports. You also must set the load-distribution method to source-based distribution, so that any given source MAC address is always sent on the same physical port.

You also can configure a single port within the group for all transmissions and use other ports for hot standby. The unused ports in the group can be swapped into operation in just a few seconds if the selected single port loses hardware-signal detection. You can configure which port is always selected for packet transmission by changing its priority with the **pagp port-priority** interface configuration command. The higher the priority, the more likely that the port will be selected.

Note The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the CLI. The **pagp learn-method** command and the **pagp port-priority** command have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.
When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. Set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. The switch then sends packets to the physical learner switch using the same port in the EtherChannel from which it learned the source address Use the **pagp learn-method** command only in this situation.

PAgP Interaction with Other Features

Cisco Discovery Protocol (CDP) sends and receives packets over the physical ports in the EtherChannel.

Note PAgP and CDP are only available on NNIs and ENIs. User network interfaces (UNIs) do not support PAgP or CDP.

Trunk ports send and receive PAgP protocol data units (PDUs) on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

PAgP sends and receives PAgP PDUs only from ports that are up and have PAgP enabled for the auto or desirable mode.

Link Aggregation Control Protocol

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

Note LACP is available only on NNIs and ENIs.

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 switch port.

LACP Modes

Table 3-2 shows the user-configurable EtherChannel LACP modes for the **channel-group** interface configuration command on an NNI or ENI.

Table 3-2 EtherChannel LACP Modes

Mode	Description
active	Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.
passive	Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.

Both the **active** and **passive LACP** modes enable ports to negotiate with partner ports to an EtherChannel based on criteria such as port speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.

Ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A port in the **active** mode can form an EtherChannel with another port that is in the **active** or **passive** mode.
- A port in the **passive** mode cannot form an EtherChannel with another port that is also in the **passive** mode because neither port starts LACP negotiation.

LACP Interaction with Other Features

The CDP sends and receives packets over the physical ports in the EtherChannel. Trunk ports send and receive LACP PDUs on the lowest numbered VLAN.

In Layer 2 EtherChannels, the first port in the channel that comes up provides its MAC address to the EtherChannel. If this port is removed from the bundle, one of the remaining ports in the bundle provides its MAC address to the EtherChannel.

LACP sends and receives LACP PDUs only from ports that are up and have LACP enabled for the active or passive mode.

EtherChannel On Mode

EtherChannel **on** mode can be used to manually configure an EtherChannel. The **on** mode forces a port to join an EtherChannel without negotiations. It can be useful if the remote device does not support PAgP or LACP. With the **on** mode, a usable EtherChannel exists only when both ends of the link are configured in the **on** mode.

Note For UNIs, the only available mode is **on**.

Ports that are configured in the **on** mode in the same channel group must have compatible port characteristics, such as speed and duplex. Ports that are not compatible are suspended, even though they are configured in the **on** mode.

Caution You should use care when using the **on** mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Load Balancing and Forwarding Methods

EtherChannel balances the traffic load across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The selected mode applies to all EtherChannels configured on the switch. You configure the load balancing and forwarding method by using the **port-channel load-balance** global configuration command.

With source-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source-MAC address of the incoming packet. Therefore, to provide load balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel.

With destination-MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the destination-host MAC address of the incoming packet. Therefore, packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

Source and Destination IP Address-Based Forwarding

With source-and-destination MAC address forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on both the source and destination MAC addresses. This forwarding method, a combination source-MAC and destination-MAC address forwarding methods of load distribution, can be used if it is not clear whether source-MAC or destination-MAC address forwarding is better suited on a particular switch. With source-and-destination MAC-address forwarding, packets sent from host A to host B, host A to host C, and host C to host B could all use different ports in the channel.

With source-IP-address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the source-IP address of the incoming packet. Therefore, to provide load-balancing, packets from different IP addresses use different ports in the channel, but packets from the same IP address use the same port in the channel.

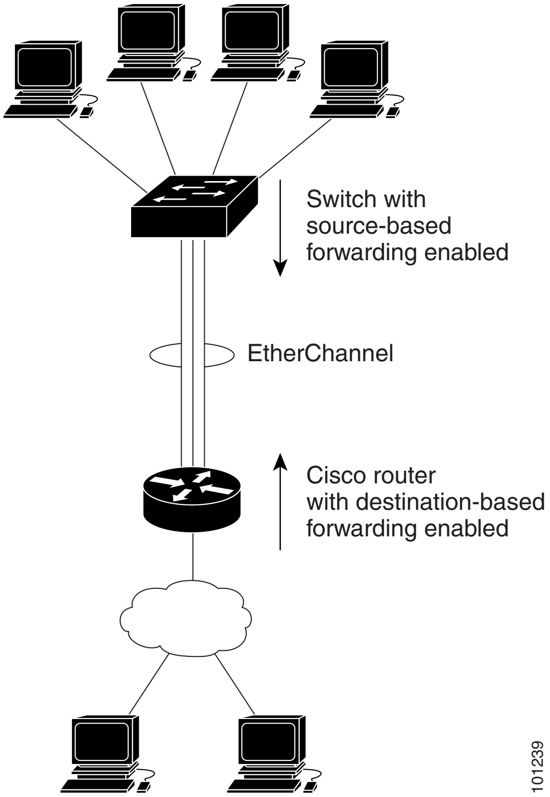
With destination-IP-address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on the destination-IP address of the incoming packet. Therefore, to provide load-balancing, packets from the same IP source address sent to different IP destination addresses could be sent on different ports in the channel. But packets sent from different source IP addresses to the same destination IP address are always sent on the same port in the channel.

With source-and-destination IP address-based forwarding, when packets are forwarded to an EtherChannel, they are distributed across the ports in the EtherChannel based on both the source and destination IP addresses of the incoming packet. This forwarding method, a combination of source-IP and destination-IP address-based forwarding, can be used if it is not clear whether source-IP or destination-IP address-based forwarding is better suited on a particular switch. In this method, packets sent from the IP address A to IP address B, from IP address A to IP address C, and from IP address C to IP address B could all use different ports in the channel.

Different load-balancing methods have different advantages, and the choice of a particular load-balancing method should be based on the position of the switch in the network and the kind of traffic that needs to be load-distributed. In Figure 3-3, an EtherChannel of four workstations communicates with a router. Because the router is a single-MAC-address device, source-based forwarding on the switch EtherChannel ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of workstations ensures that the traffic is evenly distributed from the router EtherChannel.

Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going only to a single MAC address, using the destination-MAC address always chooses the same link in the channel. Using source addresses or IP addresses might result in better load balancing.

Figure 3-3 Load Distribution and Forwarding Methods



Prerequisites

Ensure that you have all the required information to configure EtherChannels in your network.

Ensure that you have all the required information to configure Link-state Tracking in your network.

Guidelines and Limitations

EtherChannel Ports and Links

- When improperly configured, the software automatically disables some EtherChannel ports to avoid network loops and other problems. Follow these guidelines to avoid configuration problems:
  - Do not try to configure more than 48 EtherChannels on the switch.
  - Configure a PAgP EtherChannel including only NNIs or only ENIs.
  - Configure a LACP EtherChannel including only NNIs or only ENIs.
- If you configure more than eight links for an EtherChannel group, the software automatically decides which of the hot-standby ports to make active based on the LACP priority.
- Configure all ports in an EtherChannel to operate at the same speeds and duplex modes.
- All ports in an EtherChannel must be the same type, either UNI, NNI, or ENI. You cannot mix port types in an EtherChannel.
- On UNIs, the EtherChannel mode must always be configured to **On**.
- Enable all ports in an EtherChannel.
  - When you disable a port within an EtherChannel by using the **shutdown** interface configuration, the software interprets this as a link failure. As a result, the software transfers the traffic for that disabled port to one of the remaining ports in the EtherChannel.
  - UNIs and ENIs are disabled by default. NNIs are enabled by default.
- When a group is first created, all ports follow the parameters set for the first port to be added to the group. If you change the configuration of one of these parameters, you must also make the changes to all ports in the group:
  - Allowed-VLAN list
  - Spanning-tree path cost for each VLAN
  - Spanning-tree port priority for each VLAN
  - Spanning-tree Port Fast setting

Note Spanning Tree Protocol is only supported on NNIs or ENIs on which it has been specifically enabled.

- Do not configure a port to be a member of more than one EtherChannel group.
- Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

Note PAgP and LACP are only available on NNIs and ENIs.

- If the switch is running the LAN base image, you can have only four NNIs on the switch at the same time; 1therefore, only four ports in an EtherChannel can support LACP and PAgP at the same time.If the switch is running the IP services image, there is no limit to the number of NNIs that can be configured on the switch.
- Do not configure a Switched Port Analyzer (SPAN) destination port as part of an EtherChannel.

- Do not configure a secure port as part of an EtherChannel or the reverse.
- Do not configure a private-VLAN port as part of an EtherChannel.
- Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an 802.1x port. If you try to enable 802.1x on an EtherChannel port, an error message appears, and 802.1x is not enabled.
- If EtherChannels are configured on switch interfaces, remove the EtherChannel configuration from the interfaces before globally enabling 802.1x on a switch by using the **dot1x system-auth-control** global configuration command.
- Do not enable link-state tracking on individual interfaces that will be part of a downstream Etherchannel interface.

Layer 2 and Layer 3 EtherChannels

- For Layer 2 EtherChannels:
  - Assign all ports in the EtherChannel to the same VLAN, or configure them as trunks. Ports with different native VLANs cannot form an EtherChannel.
  - If you configure an EtherChannel from trunk ports, verify that the trunking mode is the same on all the trunks. Inconsistent trunk modes on EtherChannel ports can have unexpected results.
  - An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the ports do not form an EtherChannel even when PAgP is set to the **auto** or **desirable** mode.
  - NNIs or ENIs with different spanning-tree path costs can form an EtherChannel if they are otherwise compatibly configured. Setting different spanning-tree path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.
- For Layer 3 EtherChannels, assign the Layer 3 address to the port-channel logical interface, not to the physical ports in the channel.

LACP

- For systems operating with LACP, the software assigns to every link between systems a unique priority made up of these elements (listed in priority order):
  - LACP system priority
  - System ID (a combination of the LACP system priority and the switch MAC address)
  - LACP port priority
  - Port number
- In priority comparisons, numerically lower values have higher priority. The priority decides which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
- Selecting ports for active use for use in an aggregation link-priority order starts with the port attached to the highest priority link. The software selects ports for active use if the preceding higher priority selections can also be maintained. Otherwise, the software selects the port for standby mode.
- You can change the default values of the LACP system priority and the LACP port priority to affect how the software selects active and standby links.

Default Settings

Parameters	Default Setting
Channel groups	None assigned
Port-channel logical interface	None defined
PAgP mode	No default
PAgP learn method	Aggregate-port learning on all NNIs and ENIs
PAgP priority	128 on all NNIs and ENIs
LACP mode	No default
LACP learn method	Aggregate-port learning on all NNIs and ENIs
LACP port priority	32768 on all NNIs and ENIs
LACP system priority	32768

Configuring EtherChannels

- Defining Layer 2 EtherChannels, page 3-12 (required)
- Defining Layer 3 EtherChannels, page 3-15 (required)
- Configuring EtherChannel Load Balancing (Optional), page 3-19 (optional)
- Configuring the PAgP Learn Method and Priority (Optional), page 3-20 (optional)
- Configuring LACP Hot-Standby Ports, page 3-22 (optional)

Note After you configure an EtherChannel, configuration changes applied to the port-channel interface apply to all the physical ports assigned to the port-channel interface, and configuration changes applied to the physical port affect only the port to which you apply the configuration.

Defining Layer 2 EtherChannels

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify a physical port, and enter interface configuration mode. Valid interfaces include physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. **Note** If the interface is a UNI, you must enter the **port-type** {**eni** | **nni**} interface configuration command before configuring PAgP or LACP.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**switchport mode** {**access** | **trunk**} **switchport access vlan** *vlan-id*	Assign 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.

	Command	Purpose
Step 5	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	Assign the port to a channel group, and specify the PAgP or the LACP mode. For *channel-group-number*, the range is 1 to 48. **Note** For UNIs, the only available mode is **on**. For **mode**, select one of these keywords: • **auto**—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. • **desirable**—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. • **on**—Forces the port to channel without PAgP or LACP. With the **on** mode, a usable EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode. • **non-silent**—(Optional) If your switch is connected to a partner that is PAgP-capable, configure the switch port for nonsilent operation when the port is in the **auto** or **desirable** mode. If you do not specify **non-silent**, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. • **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. To remove a port from the EtherChannel group, use the **no channel-group** interface configuration command. **Note** For information on compatible modes for the switch and its partner, see the "PAgP Modes" section on page 3-5 and the "LACP Modes" section on page 3-7. To remove a port from the EtherChannel group, use the **no channel-group** interface configuration command.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove a port from the EtherChannel group, use the **no channel-group** interface configuration command.

EXAMPLE

This example shows how to configure an EtherChannel. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range fastethernet0/1 -2
Switch(config-if-range)# port-type nni
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable non-silent
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel. It assigns two ports as static-access ports in VLAN 10 to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

Defining Layer 3 EtherChannels

To configure Layer 3 EtherChannels, you create the port-channel logical interface and then put the Ethernet ports into the port-channel as described in the next two sections.

Creating Port-Channel Logical Interfaces

When configuring Layer 3 EtherChannels, you should first manually create the port-channel logical interface by using the **interface port-channel** global configuration command. Then you put the logical interface into the channel group by using the **channel-group** interface configuration command.

Note To move an IP address from a physical port to an EtherChannel, you must delete the IP address from the physical port before configuring it on the port-channel interface.

Beginning in privileged EXEC mode, follow these steps to create a port-channel interface for a Layer 3 EtherChannel. This procedure is required.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface port-channel** *port-channel-number*	Specify the port-channel logical interface, and enter interface configuration mode. For *port-channel-number*, the range is 1 to 48. **Note** To remove the port-channel, use the **no interface port-channel** *port-channel-number* global configuration command.
Step 3	**no switchport**	Put the port-channel interface into Layer 3 mode.
Step 4	**ip address** *ip-address mask*	Assign an IP address and subnet mask to the EtherChannel.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show etherchannel** *channel-group-number* **detail**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 8		Assign an Ethernet port to the Layer 3 EtherChannel. For more information. See Defining the Physical Interfaces, page 3-16.

EXAMPLE

This example shows how to create the logical port channel 5 and assign 172.10.20.10 as its IP address:

```
Switch# configure terminal
Switch(config)# interface port-channel 5
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.10.20.10 255.255.255.0
Switch(config-if)# end
```

Defining the Physical Interfaces

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify a physical port, and enter interface configuration mode. Valid interfaces include physical ports. For a PAgP EtherChannel, you can configure up to eight ports of the same type and speed for the same group. For a LACP EtherChannel, you can configure up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. **Note** If the interface is a UNI, you must enter the **port-type** {**eni** | **nni**} interface configuration command before configuring PAgP or LACP.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**no ip address**	Ensure that there is no IP address assigned to the physical port.
Step 5	**no switchport**	Put the port into Layer 3 mode.

	Command	Purpose
Step 6	**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | {**active** | **passive**}	Assign the port to a channel group, and specify the PAgP or the LACP mode. For *channel-group-number*, the range is 1 to 48. This number must be the same as the *port-channel-number* (logical port) configured in the "Creating Port-Channel Logical Interfaces" section on page 3-15. **Note** For UNIs, the only available mode is **on**. For **mode**, select one of these keywords: • **auto**—Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. • **desirable**—Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets. • **on**—Forces the port to channel without PAgP or LACP. With the **on** mode, a usable EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode. • **non-silent**—(Optional) If your switch is connected to a partner that is PAgP capable, configure the switch port for nonsilent operation when the port is in the **auto** or **desirable** mode. If you do not specify **non-silent**, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. • **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. For information on compatible modes for the switch and its partner, see the "PAgP Modes" section on page 3-5 and the "LACP Modes" section on page 3-7.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure an EtherChannel. It assigns two ports to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# no ip address
Switch(config-if-range)# no switchport
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

Configuring EtherChannel Load Balancing (Optional)

This section describes how to configure EtherChannel load balancing by using source-based or destination-based forwarding methods. For more information, see the "Load Balancing and Forwarding Methods" section on page 3-8.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}	Configure an EtherChannel load-balancing method. The default is **src-mac**. Select one of these load-distribution methods: • **dst-ip**—Load distribution is based on the destination-host IP address. • **dst-mac**—Load distribution is based on the destination-host MAC address of the incoming packet. • **src-dst-ip**—Load distribution is based on the source-and-destination host-IP address. • **src-dst-mac**—Load distribution is based on the source-and-destination host-MAC address. • **src-ip**—Load distribution is based on the source-host IP address. • **src-mac**—Load distribution is based on the source-MAC address of the incoming packet. To return EtherChannel load balancing to the default configuration, use the **no port-channel load-balance** global configuration command.
Step 3	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 4	**show etherchannel load-balance**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This section describes how to configure EtherChannel load balancing by using the source-MAC address of the incoming packet as the basis for distribution.

```
Switch# configure terminal
Switch(config)# port-channel load-balance src-mac
Switch(config)# end
```

Configuring the PAgP Learn Method and Priority (Optional)

Configures your switch as a PAgP physical-port learner and adjusts the priority so that the same port in the bundle is selected for sending packets.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

Configure EtherChannel Load Balancing. (See Configuring EtherChannel Load Balancing (Optional).)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port for transmission, and enter interface configuration mode. **Note** If the interface is a UNI, you must enter the **port-type** {**eni** | **nni**} interface configuration command before configuring LACP.

	Command	Purpose
Step 3	**pagp learn-method** physical-port	Select the PAgP learning method. By default, **aggregation-port learning** is selected, which means the switch sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives. Select **physical-port** to connect with another switch that is a physical learner. Make sure to configure the **port-channel load-balance** global configuration command to **src-mac** as described in the "Configuring EtherChannel Load Balancing (Optional)" section on page 3-19. The learning method must be configured the same at both ends of the link. If the interface is a UNI, you must enter the **port-type** {**eni** | **nni**} interface configuration command before configuring PAgP. To return the learning method to its default setting, use the **no pagp learn-method** interface configuration command.
Step 4	**pagp port-priority** *priority*	Assign a priority so that the selected port is chosen for packet transmission. For *priority*, the range is 0 to 255. The default is 128. The higher the priority, the more likely that the router chooses the port for PAgP transmission. To return the priority to its default setting, use the **no pagp port-priority** interface configuration command.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config** or **show pagp** *channel-group-number* **internal**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure the switch as a PAgP physical-port learner to adjust the priority so that the router selects the same port in the bundle for sending packets.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# pagp learn-method 3
Switch(config-if)# pagp port-priority 10
Switch(config)# end
```

Configuring LACP Hot-Standby Ports

When enabled, LACP tries to configure the maximum number of LACP-compatible ports in a channel, up to a maximum of 16 ports. Only eight LACP links can be active at one time. The software places any additional links in a hot-standby mode. If one of the active links becomes inactive, a link that is in the hot-standby mode becomes active in its place.

Note LACP is only available on NNIs and ENIs.

Configuring LACP System Priority

You can configure the system priority for all of the EtherChannels.

You cannot configure a system priority for each LACP-configured channel. By changing this value from the default, you can affect how the software selects active and standby links.

You can use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**lacp system-priority** *priority*	Configure the LACP system priority. For *priority*, the range is 1 to 65535. The default is 32768. The lower the value, the higher the system priority. **Note** To return the LACP system priority to the default value, use the **no lacp system-priority** global configuration command.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch# configure terminal
Switch(config)# lacp system-priority
Switch(config)# end
```

Configuring the LACP Port Priority

By default, all ports use the same port priority. If the local system has a lower value for the system priority and the system ID than the remote system, you can affect which of the hot-standby links become active first by changing the port priority of LACP EtherChannel ports to a lower value than the default.

Note If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), all the ports that cannot be actively included in the EtherChannel are put in the hot-standby state and are used only if one of the channeled ports fails.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode. **Note** If the interface is a UNI, you must enter the **port-type** {**eni | nni**} interface configuration command before configuring LACP.
Step 3	**lacp port-priority** *priority*	Configure the LACP port priority. For *priority*, the range is 1 to 65535. The default is 32768. The lower the value, the more likely that the port will be used for LACP transmission. To return the LACP port priority to the default value, use the **no lacp port-priority** interface configuration command.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lacp port-priority 33000
```

Verifying EtherChannel, PAgP, and LACP Configuration

To display EtherChannel, PAgP, and LACP status information, use the privileged EXEC commands described below.

Command	Description
show etherchannel [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**}	Displays EtherChannel information in a brief, detailed, and one-line summary form. Also displays the load-balance or frame-distribution scheme, port, port-channel, and protocol information. The **show etherchannel summary** display shows which ports are in the hot-standby mode (denoted with an H port-state flag).
show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	Displays LACP information such as traffic information, the internal LACP configuration, and neighbor information.
show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**}	Displays PAgP information such as traffic information, the internal PAgP configuration, and neighbor information.
show running-config	Displays the running configuration for the switch.

You can clear PAgP channel-group information and traffic counters by using the **clear pagp** {*channel-group-number* **counters** | **counters**} privileged EXEC command.

You can clear LACP channel-group information and traffic counters by using the **clear lacp** {*channel-group-number* **counters** | **counters**} privileged EXEC command.

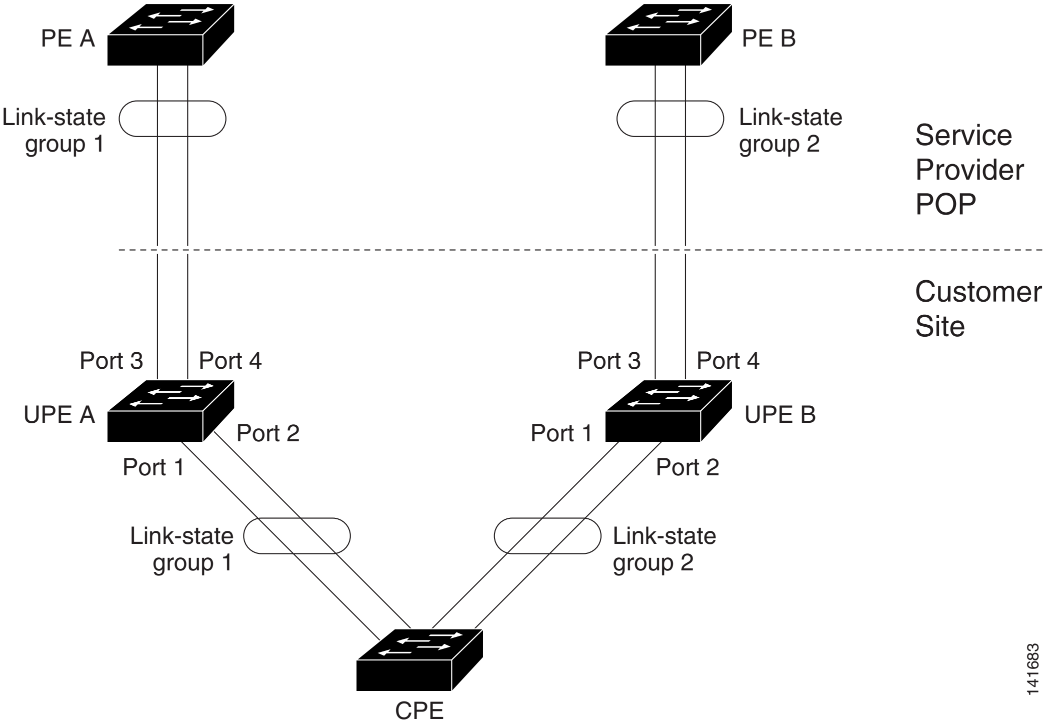
Information About Link-State Tracking

Link-state tracking, also known as trunk failover, is a feature that binds the link state of multiple interfaces. For example, link-state tracking provides redundancy in the network when used with Flex Links. If the link is lost on the primary interface, connectivity is transparently switched to the secondary interface.

As shown in Figure 3-4, Cisco IE 2000U switches are used as user-facing provider edge (UPE) switches in a customer site at the edge of the provider network connected to a customer premises equipment (CPE) switch. The UPE switches are connected to the provider edge (PE) switches in the service provider (SP) network. Customer devices, such as clients, connected to the CPE switch have multiple connections to the SP network. This configuration ensures that the traffic flow is balanced from the customer site to the SP and the reverse. Ports connected to the CPE are referred to as downstream ports, and ports connected to PE switches are referred to as upstream ports.

- UPE switch A provides links to the CPE through link-state group 1. Port 1 and port 2 are connected to the CPE. Port 3 and port 4 are connected to PE switch A through link-state group 1.
- UPE switch B provides links to the CPE through link-state group 2. Port 1 and port 2 are connected to CPE. Port 3 and 4 are connected to PE switch A through link-state group 2.

Figure 3-4 Typical Link-State Tracking Configuration



Guidelines and Limitations

- You can configure only two link-state groups per switch.
- An interface cannot be a member of more than one link-state group.

- An interface that is defined as an upstream interface cannot also be defined as a downstream interface in the same or a different link-state group. The reverse is also true.

Default Settings

Parameters	Default
Link-state Tracking	Disabled
Link-state groups	Disabled

Configuring Link-State Tracking

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**link state track** *number*	Create a link-state group, and enable link-state tracking. The group number can be 1 to 2; the default is 1. To disable a link-state group, use the **no link state track** *number* global configuration command
Step 3	**interface** *interface-id*	Specify a physical interface or range of interfaces to configure, and enter interface configuration mode. Valid interfaces include switch ports in access or trunk mode (IEEE 802.1q), routed ports, or multiple ports bundled into an upstream EtherChannel interface (static, PAgP, or LACP), also in trunk mode. Do not enable link-state tracking on individual interfaces that will be part of a downstream Etherchannel interface.
Step 4	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 5	**link state group** [*number*] {**upstream** | **downstream**}	Specify a link-state group, and configure the interface as either an **upstream** or **downstream** interface in the group.The group number can be 1 to 2; the default is 1.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to create a link-state group and configure the interfaces:

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range fastethernet/0/9 -10
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface fastethernet0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

Verifying Link-State Tracking Configuration

Command	Purpose
show link state group [*number*] **[detail]**	Displays either summary information about either all link-state groups (when you use no keywords), summary information about a specific group, or detailed information about a specific link state group.

EXAMPLE

Use the **show link state group** command to display the link-state group information. Enter this command without keywords to display information about all link-state groups. Enter the group number to display information specific to the group. Enter the detail keyword to display detailed information about the group.

This is an example of output from the **show link state group 1** command:

```
Switch> show link state group 1

Link State Group: 1      Status: Enabled, Down
```

This is an example of output from the **show link state group detail** command:

```
Switch> show link state group detail

(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled

Link State Group: 1 Status: Enabled, Down
Upstream Interfaces : Fa0/15(Dwn) Fa0/16(Dwn)
Downstream Interfaces : Fa0/11(Dis) Fa0/12(Dis) Fa0/13(Dis) Fa0/14(Dis)

Link State Group: 2 Status: Enabled, Down
Upstream Interfaces : Fa0/15(Dwn) Fa0/16(Dwn) Fa0/17(Dwn)
Downstream Interfaces : Fa0/11(Dis) Fa0/12(Dis) Fa0/13(Dis) Fa0/14(Dis)

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled
```

Configuration Example

This example shows how to create a link-state group and configure the interfaces:

```
Switch# configure terminal
Switch(config)# link state track 1
Switch(config)# interface range fastethernet/0/9 -10
Switch(config-if)# link state group 1 upstream
Switch(config-if)# interface fastethernet0/1
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/3
Switch(config-if)# link state group 1 downstream
Switch(config-if)# interface fastethernet0/5
Switch(config-if)# link state group 1 downstream
Switch(config-if)# end
```

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX

CHAPTER 4

Configuring HSRP

This chapter describes how to use the Cisco Hot Standby Router Protocol (HSRP) on the Cisco Industrial Ethernet 2000U Series Switches (IE 2000U) and Connected Grid switches, hereafter referred to as switch. HSRP provides routing redundancy for routing IP traffic without being dependent on the availability of any single router.

The switch must be running the IP services image to support HSRP.

This chapter includes the following sections:

- Information About HSRP, page 4-1
- Prerequisites, page 4-5
- Guidelines and Limitations, page 4-5
- Default Settings, page 4-6
- Configuring HSRP, page 4-6
- Verifying Configuration, page 4-13
- Feature History, page 4-14

Information About HSRP

HSRP is a 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.

HSRP 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 you configure HSRP on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that a group of configured routers share.

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; rather, it represents the common target for routers that you configure to provide backup to each other. You configure one of the routers to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address when the designated active router fails.

Note Routers in an HSRP group can be any router interface that supports HSRP, including routed ports and switch virtual interfaces (SVIs) on the switch.

HSRP provides high network availability by providing redundancy for IP traffic from hosts on networks. In a group of router interfaces, the active router is the router of choice for routing packets; and, the standby router is the router that takes over the routing duties when an active router fails or when preset conditions are met.

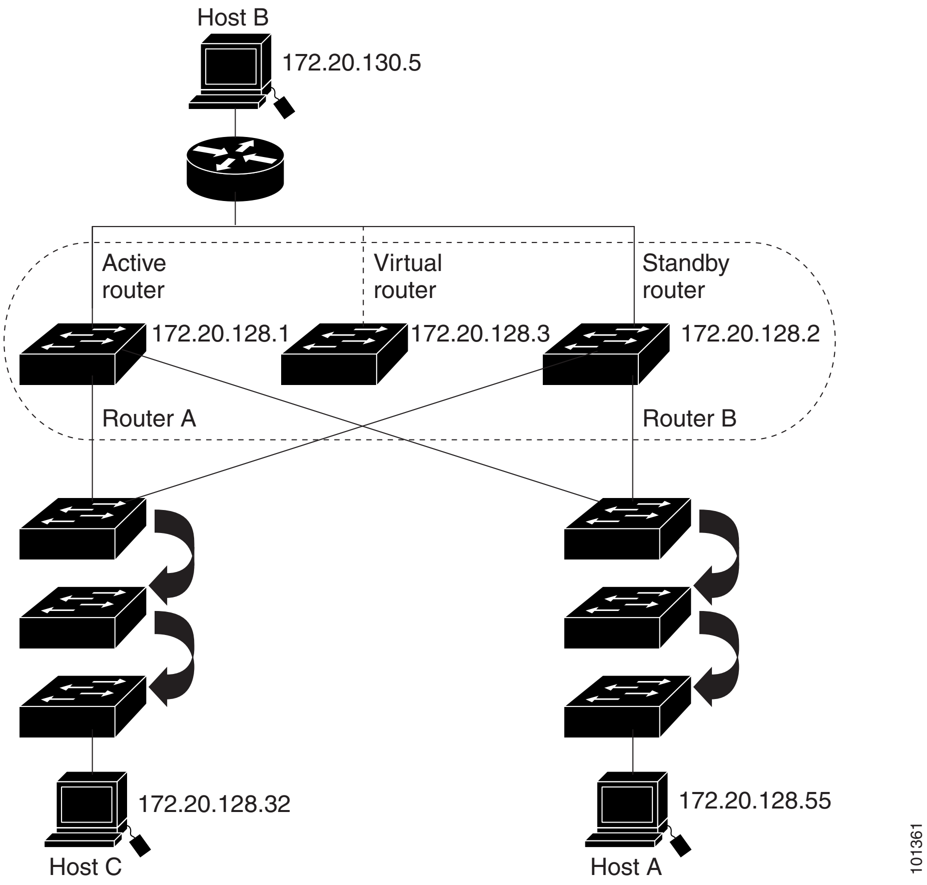
HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new router when their selected router reloads or loses power. When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among router interfaces in a group of router interfaces running HSRP. The router selected by the protocol to be the active router receives and routes packets destined for the group's MAC address. For *n* routers running HSRP, there are *n +1* IP and MAC addresses assigned.

HSRP detects when the designated active router fails, and a selected standby router assumes control of MAC and IP addresses of the Hot Standby group. A new standby router is also selected at that time. Devices running HSRP send and receive multicast UDP-based hello packets to detect router failure and to designate active and standby routers. When HSRP is configured on an interface, Internet Control Message Protocol (ICMP) redirect messages are automatically enabled for the interface.

You can configure multiple Hot Standby groups among switches that are operating in Layer 3 to make more use of the redundant routers. To do so, specify a group number for each Hot Standby command group that you configure for an interface. For example, you might configure an interface on switch 1 as an active router and one on switch 2 as a standby router and also configure another interface on switch 2 as an active router with another interface on switch 1 as its standby router.

Figure 4-1 shows a segment of a network configured for HSRP. Each router is configured with the MAC address and IP network address of the virtual router. Instead of configuring hosts on the network with the IP address of Router A, you configure them with the IP address of the virtual router as their default router. When Host C sends packets to Host B, it sends them to the MAC address of the virtual router. If for any reason, Router A stops transferring packets, Router B responds to the virtual IP address and virtual MAC address and becomes the active router, assuming the active router duties. Host C continues to use the IP address of the virtual router to address packets destined for Host B, which Router B now receives and sends to Host B. Until Router A resumes operation, HSRP allows Router B to provide uninterrupted service to users on Host C's segment that need to communicate with users on Host B's segment and also continues to perform its normal function of handling packets between the Host A segment and Host B.

Figure 4-1 Typical HSRP Configuration



HSRP Versions

The switch supports these Hot Standby Router Protocol (HSRP) versions:

- HSRPv1—Version 1 of the HSRP, the default version of HSRP. It has these features:
  - The HSRP group number can be from 0 to 255.
  - HSRPv1 uses the multicast address 224.0.0.2 to send hello packets, which can conflict with Cisco Group Management Protocol (CGMP) leave processing. You cannot enable HSRPv1 and CGMP at the same time; they are mutually exclusive.
- HSRPv2—Version 2 of the HSRP has these features:
  - To match the HSRP group number to the VLAN ID of a subinterface, HSRPv2 can use a group number from 0 to 4095 and a MAC address from 0000.0C9F.F000 to 0000.0C9F.FFFF.
  - HSRPv2 uses the multicast address 224.0.0.102 to send hello packets. HSRPv2 and CGMP leave processing are no longer mutually exclusive, and both can be enabled at the same time.
  - HSRPv2 has a different packet format than HRSPv1.

    A switch running HSRPv1 cannot identify the physical router that sent a hello packet because the source MAC address of the router is the virtual MAC address.

HSRPv2 has a different packet format than HSRPv1. A HSRPv2 packet uses the type-length-value (TLV) format and has a 6-byte identifier field with the MAC address of the physical router that sent the packet.

If an interface running HSRPv1 gets an HSRPv2 packet, the type field is ignored.

HSRPv2 and HSRPv1 are mutually exclusive. HSRPv2 is not interoperable with HSRPv1 on an interface and the reverse.

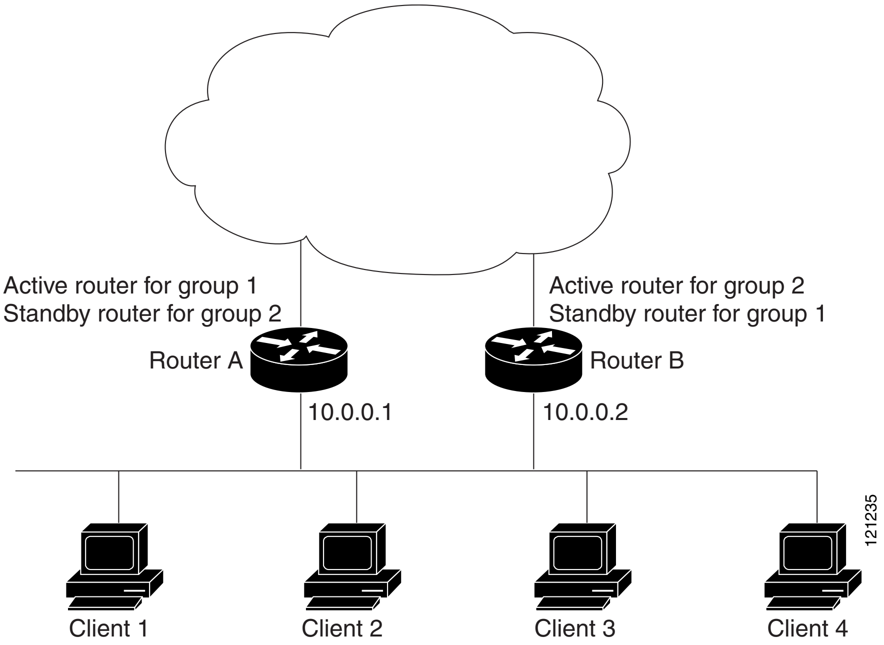
Multiple HSRP

The switch supports Multiple HSRP (MHSRP), an extension of HSRP that allows load sharing between two or more HSRP groups. You can configure MHSRP to achieve load balancing and to use two or more standby groups (and paths) from a host network to a server network. In Figure 4-2, half the clients are configured for Router A, and half the clients are configured for Router B. Together, the configuration for Routers A and B establishes two HSRP groups. For group 1, Router A is the default active router because it has the assigned highest priority, and Router B is the standby router. For group 2, Router B is the default active router because it has the assigned highest priority, and Router A is the standby router. During normal operation, the two routers share the IP traffic load. When either router becomes unavailable, the other router becomes active and assumes the packet-transfer functions of the router that is unavailable.

See the "Enabling MHSRP" section on page 4-10 for the example configuration steps.

Note For MHSRP, you need to enter the **standby preempt** interface configuration command on the HSRP interfaces so that if a router fails and then comes back up, preemption restores load sharing.

Figure 4-2 MHSRP Load Sharing


Active router for group 1
Standby router for group 2
Router A
10.0.0.1
Active router for group 2
Standby router for group 1
Router B
10.0.0.2
121235
Client 1
Client 2
Client 3
Client 4

Prerequisites

None.

Guidelines and Limitations

HSRP Interfaces

- You can configure HSRP on a maximum of 32 VLAN or routing interfaces.
- A specified interface must be one of these Layer 3 interfaces:
  - Routed port: a physical port configured as a Layer 3 port by entering the **no switchport** interface configuration command.
  - SVI: a VLAN interface created by using the **interface vlan** *vlan_id* global configuration command and by default a Layer 3 interface.
  - Etherchannel port channel in Layer 3 mode: a port-channel logical interface created by using the **interface port-channel** *port-channel-number* global configuration command and binding the Ethernet interface into the channel group. For more information, see the "Defining Layer 3 EtherChannels" section on page 3-15.
- All Layer 3 interfaces must have IP addresses assigned to them.

HSRPv1 and HSRPv2 on the Same Switch

- You configure HSRPv2 and HSRPv1 on the same switch when you configure HSRPv2 on different interfaces than those on which you configure HSRPv1.
- You can change the version of an HSRP group from HSRPv2 to HSRPv1 only when the group number is less than 256.
- If you change the HSRP version on an interface, each HSRP group resets because it now has a new virtual MAC address.

HSRP Priority

- Assigning a priority allows you to select the active and standby routers. If preemption is enabled, the router with the highest priority becomes the active router. If priorities are equal, the current active router does not change.
- The highest number (1 to 255) represents the highest priority (most likely to become the active router).
- When setting the priority, preempt, or both, you must specify at least one keyword (**priority**, **preempt**, or both).
- The priority of the device can change dynamically if an interface is configured with the **standby track** command and another interface on the router goes down.
- The **standby track** interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.

- The **standby track** *interface-priority* interface configuration command specifies how much to decrement the hot standby priority when a tracked interface goes down. When the interface comes back up, the priority is incremented by the same amount.
- When multiple tracked interfaces are down and *interface-priority* values have been configured, the configured priority decrements are cumulative. If tracked interfaces that were not configured with priority values fail, the default decrement is 10, and it is noncumulative.
- When routing is first enabled for the interface, it does not have a complete routing table. If it is configured to preempt, it becomes the active router, even though it is unable to provide adequate routing services. To solve this problem, configure a delay time to allow the router to update its routing table.

HSRP Authentication and Timers

- The authentication string is sent unencrypted in all HSRP messages. You must configure the same authentication string on all routers and access servers on a cable to ensure interoperation. Authentication mismatch prevents a device from learning the designated Hot Standby IP address and timer values from other routers configured with HSRP.
- Routers or access servers on which standby timer values are not configured can learn timer values from the active or standby router. The timers configured on an active router always override any other timer settings.
- All routers in a Hot Standby group should use the same timer values. Normally, the *holdtime* is greater than or equal to 3 times the *hellotime*.

Default Settings

Parameters	Description
HSRP version	Version 1
HSRP groups	None configured
Standby group number	0
Standby MAC address	System assigned as: 0000.0c07.acXX, where *XX* is the HSRP group number
Standby priority	100
Standby delay	0 (no delay)
Standby track interface priority	10
Standby hello time	3 seconds
Standby holdtime	10 seconds

Configuring HSRP

This section includes the following topics:

- Enabling HSRP, page 4-7
- Defining HSRP Priority, page 4-8
- Enabling MHSRP, page 4-10

- Defining HSRP Authentication and Timers, page 4-11
- Enabling HSRP Support for ICMP Redirect Messages, page 4-13

Enabling HSRP

Note The **standby ip** interface configuration command activates HSRP on the configured interface.

- When you specify an IP address, the router uses that address as the designated address for the Hot Standby group.
- When you do not specify an IP address, the router learns the address through the standby function.

You must configure at least one Layer 3 port on the LAN with the designated address. Configuring an IP address always overrides another designated address currently in use.

If you enable the **standby ip** command on a router interface and enable proxy ARP on that same interface, then proxy ARP requests are answered using the Hot Standby group MAC address when Hot Standby state is active on the interface. If the interface is in a different state, the router suppresses proxy ARP responses.

BEFORE YOU BEGIN

Review the Guidelines and Limitations for this feature. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the Layer 3 interface on which you want to enable HSRP.
Step 3	**no shutdown**	Enable the port, if necessary. By default, user network interfaces (UNIs) and enhanced network interfaces (ENIs) are disabled, and network node interfaces (NNIs) are enabled.
Step 4	**no switchport**	If necessary, disable Layer 2 switching on the port to enable the Layer 3 interface.
Step 5	**standby version** {**1** | **2**}	(Optional) Configure the HSRP version on the interface. • 1— Select HSRPv1 • 2— Select HSRPv2 If you do not enter this command or do not specify a keyword, then the interface runs the default HSRP version, HSRP v1.

	Command	Purpose
Step 6	**standby** [*group-number*] **ip** [*ip-address* [**secondary**]]	Create (or enable) the HSRP group using its number and virtual IP address. • (Optional) *group-number*—The HSRP group number that you want to enable on the interface. The range is 0 to 255; the default is 0. If there is only one HSRP group, you do not need to enter a group number. • (Optional on all but one interface) *ip-address*—The virtual IP address of the hot standby router interface. You must enter the virtual IP address for at least one of the interfaces. The virtual IP address can be learned on the other interfaces. • (Optional) **secondary**—The IP address is a secondary hot standby router interface. When you do not designate either router as a secondary or standby router and no priorities are set, the router compares the primary IP addresses and the higher IP address becomes the active router. The next highest IP address becomes the standby router. Use the **no standby** [*group-number*] **ip** [*ip-address*] interface configuration command to disable HSRP
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show standby** [*interface-id* [*group*]]	Verify the configuration.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to activate HSRP for group 1 on an interface. The IP address used by the hot standby group is learned by using HSRP.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# end
Switch# show standby
```

Defining HSRP Priority

HSRP Priority sets the characteristics for finding active and standby routers. It also defines the behavior for the standby router when it becomes the active router.

BEFORE YOU BEGIN

Review the HSRP Priority Guidelines and Limitations. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the HSRP interface on which you want to set priority.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	**standby** [*group-number*] **priority** *priority*	Set a **priority** value used in choosing the active router. The range is 1 to 255; the default priority is 100. The highest number represents the highest priority. • (Optional) *group-number*—The group number to which the command applies. Use the **no** form of the command to restore the default values.
Step 5	**standby** [*group-number*] **preempt** [**delay** [**minimum** *seconds*] [**reload** *seconds*] [**sync** *seconds*]]	Configure the router to **preempt**, which means that when the local router has a higher priority than the active router, it becomes the active router. • (Optional) *group-number*—The group number to which the command applies. • (Optional) **delay minimum**—Set to cause the local router to postpone taking over the active role for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over). • (Optional) **delay reload**—Set to cause the local router to postpone taking over the active role after a reload for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over after a reload). • (Optional) **delay sync**—Set to cause the local router to postpone taking over the active role so that IP redundancy clients can reply (either with an *ok* or *wait* reply) for the number of seconds shown. The range is 0 to 36000 seconds (1 hour); the default is 0 (no delay before taking over). Use the **no** form of the command to restore the default values.

	Command	Purpose
Step 6	**standby** [*group-number*] **track** *type number* [*interface-priority*]	Configure an interface to track other interfaces so that if one of the other interfaces goes down, the device's Hot Standby priority is lowered. • (Optional) *group-number*—The group number to which the command applies. • *type*—Enter the interface type (combined with interface number) that is tracked. • *number*—Enter the interface number (combined with interface type) that is tracked. • (Optional) *interface-priority*—Enter the amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up. The default value is 10. Use the **no** form of the command to restore the default values.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify the configuration of the standby groups.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example activates a port, sets an IP address and a priority of 120 (higher than the default value), and waits for 300 seconds (5 minutes) before attempting to become the active router:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby ip 172.20.128.3
Switch(config-if)# standby priority 120 preempt delay 300
Switch(config-if)# end
```

Enabling MHSRP

To enable MHSRP and load balancing, you must configure two routers as active routers for their groups, with virtual routers as standby routers. This example shows how to enable the MHSRP configuration shown in Figure 4-2. You need to enter the **standby preempt** interface configuration command on each HSRP interface so that if a router fails and comes back up, the preemption occurs and restores load balancing.

Router A is configured as the active router for group 1, and Router B is configured as the active router for group 2. The HSRP interface for Router A has an IP address of 10.0.0.1 with a group 1 standby priority of 110 (the default is 100). The HSRP interface for Router B has an IP address of 10.0.0.2 with a group 2 standby priority of 110.

Group 1 uses a virtual IP address of 10.0.0.3 and group 2 uses a virtual IP address of 10.0.0.4.

Note For detailed configuration steps, refer to Enabling HSRP and Defining HSRP Priority.

EXAMPLE

Router A Configuration

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.1 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 priority 110
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

Router B Configuration

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 10.0.0.2 255.255.255.0
Switch(config-if)# standby 1 ip 10.0.0.3
Switch(config-if)# standby 1 preempt
Switch(config-if)# standby 2 ip 10.0.0.4
Switch(config-if)# standby 2 priority 110
Switch(config-if)# standby 2 preempt
Switch(config-if)# end
```

Defining HSRP Authentication and Timers

You can optionally configure an HSRP authentication string or change the hello-time interval and holdtime.

BEFORE YOU BEGIN

Review the HSRP Authentication and Timers Guidelines and Limitations. (See Guidelines and Limitations.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the HSRP interface on which you want to set authentication.
Step 3	**no shutdown**	Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.

	Command	Purpose
Step 4	**standby** [*group-number*] **authentication** *string*	(Optional) **authentication** *string*—Enter a string to be carried in all HSRP messages. The authentication string can be up to eight characters in length; the default string is **cisco.** • (Optional) *group-number*—The group number to which the command applies. Use the **no standby** [*group-number*] **authentication** *string* interface configuration command to delete an authentication string.
Step 5	**standby** [*group-number*] **timers** *hellotime holdtime*	(Optional) Configure the time between hello packets and the time before other routers declare the active router to be down. • *group-number*—The group number to which the command applies. • *hellotime*—The hello interval in seconds. The range is from 1 to 255; the default is 3 seconds. • *holdtime*—The time in seconds before the active or standby router is declared to be down. The range is from 1 to 255; the default is 10 seconds. Use the **no standby** [*group-number*] **timers** *hellotime holdtime* interface configuration command to restore timers to their default values.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify the configuration of the standby groups.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

EXAMPLE

This example shows how to configure *word* as the authentication string required to allow Hot Standby routers in group 1 to interoperate:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 authentication word
Switch(config-if)# end
```

This example shows how to set the timers on standby group 1 with the time between hello packets at 5 seconds and the time after which a router is considered down to be 15 seconds:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# standby 1 ip
Switch(config-if)# standby 1 timers 5 15
Switch(config-if)# end
```

Enabling HSRP Support for ICMP Redirect Messages

When you configure HSRP on an interface, the router automatically enables Internet Control Message Protocol (ICMP) redirect messages on those interfaces.

This feature filters outgoing ICMP redirect messages through HSRP, in which the next hop IP address might be changed to an HSRP virtual IP address. ICMP is a network layer Internet protocol that provides message packets to report errors and other information relevant to IP processing. ICMP provides diagnostic functions, such as sending and directing error packets to the host.

When the switch is running HSRP, make sure hosts do not discover the interface (or real) MAC addresses of routers in the HSRP group. If a host is redirected by ICMP to the real MAC address of a router and that router later fails, packets from the host are lost.

Verifying Configuration

Command	Purpose
show standby [*interface-id* [*group*]] [**brief**] [**detail**]	You can display HSRP information for the whole switch, for a specific interface, for an HSRP group, or for an HSRP group on an interface. You can also specify whether to display a concise summary (brief) of HSRP information or detailed HSRP information. The default display is **detail**. If there are a large number of HSRP groups, using the **show standby** command without qualifiers can result in a large display.

This is a an example of output from the **show standby** privileged EXEC command, displaying HSRP information for two standby groups (group 1 and group 100):

```
Switch# show standby
VLAN1 - Group 1
   Local state is Standby, priority 105, may preempt
   Hellotime 3 holdtime 10
   Next hello sent in 00:00:02.182
   Hot standby IP address is 172.20.128.3 configured
   Active router is 172.20.128.1 expires in 00:00:09
   Standby router is local
   Standby virtual mac address is 0000.0c07.ac01
   Name is bbb
VLAN1 - Group 100
   Local state is Active, priority 105, may preempt
   Hellotime 3 holdtime 10
   Next hello sent in 00:00:02.262
   Hot standby IP address is 172.20.138.51 configured
   Active router is local
   Standby router is unknown expired
   Standby virtual mac address is 0000.0c07.ac64
   Name is test
```

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520 switch	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX