Configuring Fallback Bridging

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Fallback Bridging

- Up to 32 bridge groups can be configured on the switch.
- An interface (an SVI or routed port) can be a member of only one bridge group.
- Use a bridge group for each separately bridged (topologically distinct) network connected to the switch.
- Do not configure fallback bridging on a switch configured with private VLANs.
- All protocols except IP (Version 4 and Version 6), Address Resolution Protocol (ARP), reverse ARP(RARP), LOOPBACK, Frame Relay ARP, and shared STP packets are fallback bridged.

Related Topics

Changing the VLAN Bridge Spanning Tree Priority, on page 5
Changing the Interface Priority, on page 7
Assigning Path Cost, on page 8
Adjusting the Intervals Between Hello BPDUs, on page 9
Changing the Forward-Delay Interval, on page 10
Changing the Maximum-Idle Interval, on page 12

Information about Fallback Bridging

Fallback Bridging Overview

With fallback bridging, the switch bridges together two or more VLANs or routed ports, essentially connecting multiple VLANs within one bridge domain. Fallback bridging forwards traffic that the switch does not route and forwards traffic belonging to a nonroutable protocol such as DECnet. A VLAN bridge domain is represented with switch virtual interfaces (SVIs). A set of SVIs and routed ports (which do not have any VLANs associated with them) can be configured (grouped together) to form a bridge group. Recall that an SVI represents a VLAN of switch ports as one interface to the routing ports (which do not have any VLANs associated with them) can be configured (grouped together) to form a bridge group. Recall that an SVI represents a VLAN of switch ports as one interface to the routing or bridging function in the system. You associate only one SVI with a VLAN, and you configure an SVI for a VLAN only when you want to route between VLANs, to fallback-bridge nonroutable protocols between VLANs, or to provide IP host connectivity to the switch. A routed port is a physical port that acts like a port on a router, but it is not connected to a router. A routed port is not associated with a particular VLAN, does not support VLAN subinterfaces, but behaves like a normal routed port.

A bridge group is an internal organization of network interfaces on a switch. You cannot use bridge groups to identify traffic switched within the bridge group outside the switch on which they are defined. Bridge groups on the switch function as distinct bridges; that is, bridged traffic and bridge protocol data units (BPDUs) are not exchanged between different bridge groups on a switch.

Fallback bridging does not allow the spanning trees from the VLANs being bridged to collapse. Each VLAN has its own spanning-tree instance and a separate spanning tree, called the VLAN-bridge spanning tree, which runs on top of the bridge group to prevent loops.

The switch creates a VLAN-bridge spanning-tree instance when a bridge group is created. The switch runs the bridge group and treats the SVIs and routed ports in the bridge group as its spanning-tree ports.

These are the reasons for placing network interfaces into a bridge group:

- To bridge all non-routed traffic among the network interfaces making up the bridge group. If the packet destination address is in the bridge table, the packet is forwarded on a single interface in the bridge group. If the packet destination address is not in the bridge table, the packet is flooded on all forwarding interfaces in the bridge group. A source MAC address is learned on a bridge group only when the address is learned on a VLAN (the reverse is not true). Any address that is learned on a stack member is learned by all switchesin the stack.
- To participate in the spanning-tree algorithm by receiving, and in some cases sending, BPDUs on the LANs to which they are attached. A separate spanning-tree process runs for each configured bridge group. Each bridge group participates in a separate spanning-tree instance. A bridge group establishes a spanning-tree instance based on the BPDUs it receives on only its member interfaces. If the bridge STP BPDU is received on a port whose VLAN does not belong to a bridge group, the BPDU is flooded on all the forwarding ports of the VLAN.

Fallback Bridging and Switching Stacks

When the stack master fails, a stack member becomes the new stack master by using the election process. The new stack master creates new VLAN-bridge spanning-tree instance, which temporarily puts the spanning-tree ports used for fallback bridging into a non-forwarding state. A momentary traffic disruption

occurs until the spanning-tree states transition to the forwarding state. All MAC addresses must be relearned in the bridge group.

Note If a stack master running the IP Services feature set fails and if the newly elected stack master is running the IP Base feature set, theswitch stack loses its fallback bridging capability.

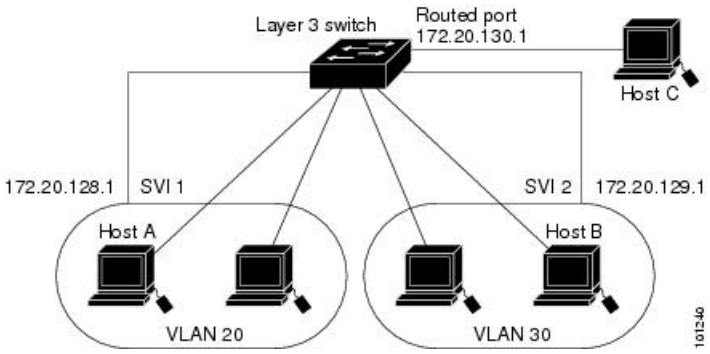
If stacks merge or if a switch is added to the stack, any new VLANs that are part of a bridge group and become active are included in the VLAN-bridge STP.

When a stack member fails, the addresses learned from this member are deleted from the bridge group MAC address table.

Example: Fallback Bridging Network

The following figure shows a fallback bridging network example. The switch has two ports configured as SVIs with different assigned IP addresses and attached to two different VLANs. Another port is configured as a routed port with its own IP address. If all three of these ports are assigned to the same bridge group, non-IP protocol frames can be forwarded among the end stations connected to the switch even though they are on different networks and in different VLANs. IP addresses do not need to be assigned to routed ports or SVIs for fallback bridging to work.

Figure 1: Fallback Bridging Network Example



How to Configure Fallback Bridging

Creating a Bridge Group

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

Note The protected port feature is not compatible with fallback bridging. When fallback bridging is enabled, it is possible for packets to be forwarded from one protected port on to another protected port on the same switch if the ports are in different VLANs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **bridge** *bridge-group***priority***number*
4. **interface***interface -id*
5. **bridge-group** *bridge-group*
6. **show running-config**
7. **copy running-config startup-config**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**bridge** *bridge-group***priority***number* **Example:** `Switch(config)# bridge 10 protocol vlan-bridge`	Assign a bridge group number, and specify the VLAN-bridge spanning-tree protocol to run in the bridge group. The **ibm** and **dec** keywords are not supported. For bridge-group, specify the bridge group number. The range is 1 to 255. You can create up to 32 bridge groups. Frames are bridged only among interfaces in the same group.
Step 4	**interface***interface -id* **Example:** `Switch(config)# interface gigabitethernet3/0/1`	Specify the interface on which you want to assign the bridge group, and enter interface configuration mode. The specified interface must be one of these: • A routed port: a physical port that you have configured as a Layer 3 port by entering the no switchport interface configuration command. • An SVI: a VLAN interface that you created by using the **interface vlan***vlan-id* global configuration command. **Note** You can assign an IP address to the routed port or to the SVI, but it is not required.

	Command or Action	Purpose
Step 5	**bridge-group** *bridge-group* **Example:** `Switch(config)# bridge-group 10`	Assign a bridge group number, and specify the VLAN-bridge spanning-tree protocol to run in the bridge group. The **ibm** and **dec** keywords are not supported. For bridge-group, specify the bridge group number. The range is 1 to 255. You can create up to 32 bridge groups. Frames are bridged only among interfaces in the same group.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 8	**end**	Returns to privileged EXEC mode.

Adjusting Spanning Tree Parameters

You might need to adjust certain spanning-tree parameters if the default values are not suitable. You configure parameters affecting the entire spanning tree by using variations of the bridge global configuration command. You configure interface-specific parameters by using variations of the bridge-group interface configuration command.

Note Only network administrators with a good understanding of how switchesand STP function should make adjustments to spanning-tree parameters. Poorly planned adjustments can have a negative impact on performance. A good source on switching is the IEEE 802.1D specification.

Changing the VLAN Bridge Spanning Tree Priority

You can globally configure the VLAN-bridge spanning-tree priority of a switch when it ties with another switch for the position as the root switch. You also can configure the likelihood that the switch will be selected as the root switch. Follow these steps to change the switch priority. This procedure is optional.

SUMMARY STEPS

1. **enable**
2.
3. **configure terminal**
4. **bridge** *bridge-group***priority***number*
5. **end**

6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2		
Step 3	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 4	**bridge** *bridge-group* **priority** *number* **Example:** `Switch(config)# bridge 10 priority 100`	Changes the VLAN-bridge spanning-tree priority of the Switch. • For bridge-group, specify the bridge group number. The range is 1 to 255. • For number, enter a number from 0 to 65535. The default is 32768. The lower the number, the more likely the Switch will be chosen as the root.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Restrictions for Fallback Bridging, on page 1
Default Fallback Bridging Configuration, on page 14

Changing the Interface Priority

You can change the priority for a port. When two switches tie for position as the root switch, you configure a port priority to break the tie. The switch with the lowest interface value is elected. Follow these steps to change the interface priority. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **bridge-group** *bridge-group***priority***number*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	
Step 4	**bridge-group** *bridge-group***priority***number* **Example:** `Switch(config)# bridge-group 10 priority 20`	Changes the VLAN-bridge spanning-tree priority of the switch. • For bridge-group, specify the bridge group number. The range is 1 to 255. • For number, enter a number from 0 to 255 in increments of 4. The lower the number, the more likely that the port on the switch will be chosen as the root. The default is 128.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:**	Verifies your entries.

	Command or Action	Purpose
	`Switch# show running-config`	
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Restrictions for Fallback Bridging, on page 1
Default Fallback Bridging Configuration, on page 14

Assigning Path Cost

Each port has a path cost associated with it. By convention, the path cost is 1000/data rate of the attached LAN, in Mb/s. Follow these steps to assign a path cost. This procedure is optional.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	

	Command or Action	Purpose
Step 4	**bridge-group** *bridge-group***path cost***cost* **Example:** `Switch(config)# bridge-group 10 path-cost 20`	Assigns the path cost of a port. • For bridge-group, specify the bridge group number. The range is 1 to 255. • For cost, enter a number from 0 to 65535. The higher the value, the higher the cost. • For 10 Mb/s, the default path cost is 100. • For 100 Mb/s, the default path cost is 19. • For 1000 Mb/s, the default path cost is 4.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Restrictions for Fallback Bridging, on page 1
Default Fallback Bridging Configuration, on page 14

Adjusting BPDU Intervals

Adjusting the Intervals Between Hello BPDUs

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

Follow these steps to adjust the interval between hello BPDUs. This procedure is optional.

SUMMARY STEPS

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

6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**bridge** *bridge-group***hello-time***seconds* **Example:** `Switch(config)# bridge 10 hello-time 5`	Specifies the interval between hello BPDUs. • For bridge-group, specify the bridge group number. The range is 1 to 255. • For seconds, enter a number from 1 to 10. The default is 2.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Restrictions for Fallback Bridging, on page 1
Default Fallback Bridging Configuration, on page 14

Changing the Forward-Delay Interval

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

Follow these steps to change the forward-delay interval. This procedure is optional.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**bridge** *bridge-group***forward-time***seconds* **Example:** `Switch(config)# bridge 10 forward-time 10`	Specifies the forward-time interval. • For bridge-group, specify the bridge group number. The range is 1 to 255. • For seconds, enter a number from 4 to 200. The default is 20.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Restrictions for Fallback Bridging, on page 1
Default Fallback Bridging Configuration, on page 14

Changing the Maximum-Idle Interval

If a switch does not receive BPDUs from the root switch within a specified interval, it re-computes the spanning-tree topology.

Follow these steps to change the maximum-idle interval (maximum aging time). This procedure is optional.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**bridge** *bridge-group***max-age***seconds* **Example:** `Switch(config)# bridge 10 max-age 30`	Specifies the interval that the switch waits to hear BPDUs from the root switch. • For bridge-group, specify the bridge group number. The range is 1 to 255. • For seconds, enter a number from 6 to 200. The default is 30.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

Related Topics

Restrictions for Fallback Bridging, on page 1
Default Fallback Bridging Configuration, on page 14

Disabling the Spanning Tree on an Interface

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

Follow these steps to disable spanning tree on a port. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **bridge-group** *bridge-group***priority***spanning-disabled*
5. **show running-config**
6. **copy running-config startup-config**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet2/0/1`	
Step 4	**bridge-group** *bridge-group***priority***spanning-disabled*	Disables spanning tree on the port.

	Command or Action	Purpose
	Example: `Switch(config)# bridge group 10 spanning-disabled`	For bridge-group, specify the bridge group number. The range is 1 to 255.
Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 7	**end**	Returns to privileged EXEC mode.

Monitoring and Maintaining Fallback Bridging

Table 1: Commands for Monitoring and Maintaining Fallback Bridging

Command	Purpose
clear bridge *bridge-group*	Removes any learned entries from the forwarding database.
show bridge*[bridge-group]* **group**	Displays details about the bridge group.
show bridge *[bridge-group] interface-id\mac -address*|**verbose**	Displays MAC addresses learned in the bridge group.

Default Fallback Bridging Configuration

Table 2: Default Fallback Bridging Configuration

Feature	Default Setting
Bridge groups	None are defined or assigned to a port. No VLAN-bridge STP is defined.
Switch forwards frames for stations that it has dynamically learned	Enabled
Switch priority	32768
Port priority	128

Feature	Default Setting
Port path cost	• 10 Mb/s: 100 • 100 Mb/s: 19 • 1000 Mb/s: 4
Hello BPDU interval	2 seconds
Forward-delay interval	20 seconds
Maximum-idle interval	30 seconds

Related Topics

Changing the VLAN Bridge Spanning Tree Priority, on page 5
Changing the Interface Priority, on page 7
Assigning Path Cost, on page 8
Adjusting the Intervals Between Hello BPDUs, on page 9
Changing the Forward-Delay Interval, on page 10
Changing the Maximum-Idle Interval, on page 12

Additional References for Fallback Bridging

Standards and RFCs

Standard/RFC	Title
RFC 1757	Remote Network Monitoring Management

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support