Configuring VLANs

This chapter describes how to configure your access point to operate with the VLANs set up on your wired LAN.

Understanding VLANs

A VLAN is a switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

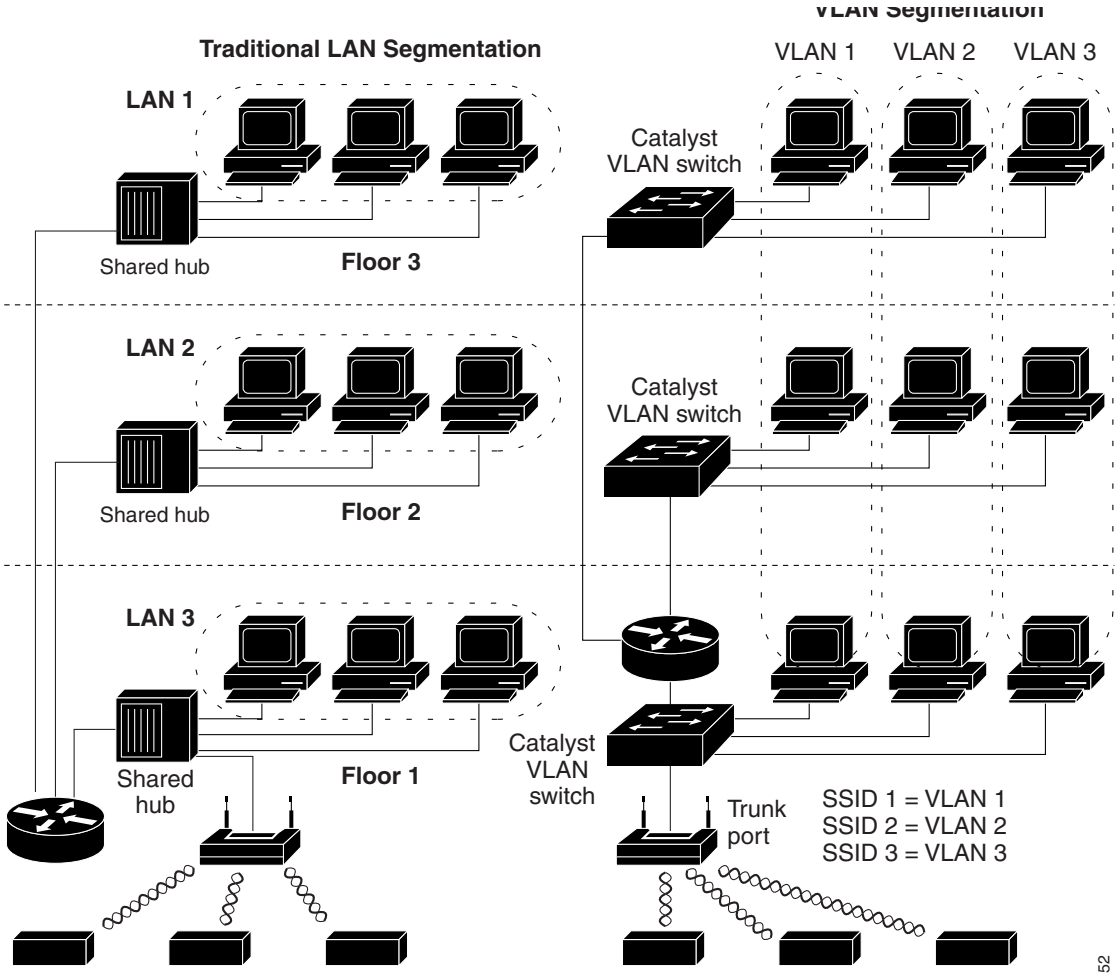
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

You extend VLANs into a wireless LAN by adding IEEE 802.1Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different SSIDs. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated to an SSID mapped to a certain VLAN are 802.1Q tagged before they are forwarded onto the wired network.

Figure 14-1 shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 14-1 LAN and VLAN Segmentation with Wireless Devices



For more information on VLAN design and configuration, see the Cisco IOS Switching Services Configuration Guide at the following URL:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c.html

Incorporating Wireless Devices into VLANs

The basic wireless components of a VLAN consist of an access point and a client associated to it using wireless technology. The access point is physically connected through a trunk port to the network VLAN switch on which VLANs are configured. The physical connection to the VLAN switch is through the access point's Ethernet port.

In fundamental terms, the key to configuring an access point to connect to a specific VLAN is to configure its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID or name, it follows that if the SSID on an access point is configured to recognize a specific VLAN ID or name, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID can access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. You can configure up to 16 SSIDs on your access point, so you can support up to 16 VLANs.

You can assign more than one SSID to a given VLAN. However, a given SSID can be mapped to only one VLAN. Also, the SSID to VLAN mapping must be unique per interface.

For example, you configure SSID1 and SSID2. If you assign SSID1 to VLANA on radio 0, then you cannot assign SSID2 to VLANA on the same radio 0. You can assign SSID2 to VLANA on radio 1. Alternatively, you can assign SSID2 to VLANB on radio 0 or on radio 1 or on both. If you assign SSID2 to VLANB on radio 0, you can assign SSID2 to radio 1, but it must also be assigned to VLANB. You cannot assign SSID2 (or SSID1) to VLANA on radio 0, and to VLANB on radio 1.

You can use the VLAN feature to deploy wireless devices with greater efficiency and flexibility. For example, one access point can now handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple access points would have to be employed to serve classes of users based on the access and permissions they were assigned.

These are two common strategies for deploying wireless VLANs:

- Segmentation by user groups: You can segment your wireless LAN user community and enforce a different security policy for each user group. For example, you can create three wired and wireless VLANs in an enterprise environment for full-time and part-time employees and also provide guest access.
- Segmentation by device types: You can segment your wireless LAN to allow different devices with different security capabilities to join the network. For example, some wireless users might have handheld devices that support only support only pre-shared key (PSK) security mechanisms, and some wireless users might have more sophisticated devices using 802.1x/EAP. You can group and isolate these devices into separate VLANs.

Repeaters cannot repeat SSIDs mapped to a VLAN. When configuring a root access point and a repeater, make sure that the SSID on the root AP and the same SSID on the repeater use the native VLAN. You can configure other SSIDs on the root AP and the repeater AP that would be mapped to a VLAN, but these tagged SSIDs cannot be repeated.

When configuring a bridge to non-root bridge link, the SSID used on the bridge must be untagged (use the native VLAN). You can also configure other SSIDs on both the root bridge AP and the non-root bridge AP that would be mapped to a VLAN. These SSIDs will be forwarded between the root bridge and the non-root bridge through the SSID associated to the native VLAN.

Configuring VLANs

These sections describe how to configure VLANs on your access point:

Configuring a VLAN

Configuring your access point to support VLANs is a three-step process:

1. Enable the VLAN on the radio and Ethernet ports.
   Enabling the VLAN on the radio and Ethernet ports also creates the VLANs in the access point configuration.
2. Create an SSID, and assign it to a VLAN.
3. Assign encryption settings to a VLAN on a given radio interface.

This section describes how to assign SSIDs to VLANs and how to enable a VLAN on the access point radio and Ethernet ports. For detailed instructions on assigning authentication types to SSIDs, see Chapter 11, "Configuring Authentication Types." For instructions on assigning other settings to SSIDs, see Chapter 7, "Configuring Multiple SSIDs."

You can configure up to 16 SSIDs on the access point, so you can support up to 16 VLANs that are configured on your LAN.

Step 1 - Enabling the VLAN on the radio and Ethernet ports

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN and enable the VLAN on the access point radio and Ethernet ports.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio 0.x | 1.x**	Enter interface configuration mode for the radio VLAN sub interface.
Step 3	**encapsulation dot1q** *vlan-id* [**native**]	Enable a VLAN on the radio interface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 4	**exit**	Return to global configuration mode.

Step 2 - Creating an SSID and assigning it to a VLAN

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN.

	Command	Purpose
Step 1	**dot11 ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. **Note** You use the **ssid** command's authentication options to configure an authentication type for each SSID. See Chapter 11, "Configuring Authentication Types," for instructions on configuring authentication types.
Step 2	**vlan** *vlan-id*	(Optional) Assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. Enter a VLAN ID from 1 to 4095. You can assign only one VLAN to an SSID, but you can assign two SSIDs to a VLAN, as long as each SSID is sent to a different radio interface. However, you cannot assign two SSIDs to the same VLAN on the same interface. **Tip** If your network uses VLAN names, you can also assign names to the VLANs on your access point. See the "Assigning Names to VLANs" section on page 14-7 for instructions.
Step 3	**exit**	Return to interface configuration mode for the radio interface.

Step 3 - Assigning encryption settings to a VLAN on a given radio interface

Beginning in privileged EXEC mode, follow these steps to assign encryption settings to a VLAN on a given radio interface.

	Command	Purpose
Step 1	**interface dot11radio 0 | 1**	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 2	**ssid** *ssid-string*	Assigns the SSID to the interface.
Step 3	**encryption vlan** *vlan-id* **{mode | key}**	Configures the encryption method for the VLAN associated to this interface. For more details see Chapter 10, "Configuring WLAN Authentication and Encryption,"which describes in detail the possible methods and keys.

The following example shows how to:

- Enable a VLAN on the radio and ethernet ports as the native VLAN

- Assign an SSID to a VLAN
- Assign an AES-CCMP encryption method to a VLAN
- Assign an SSID to a radio interface

```
ap# configure terminal
ap(config)# interface dot11Radio 0.31
ap(config-subif)# encapsulation dot1Q 31 native
ap(config-subif)# exit
ap(config)# interface gigabitEthernet 0.31
ap(config-subif)# encapsulation dot1Q 31 native
ap(config-subif)# exit
ap(config)# dot11 ssid batman
ap(config-ssid)# vlan 31
ap(config-ssid)# exit
ap(config)# interface dot11Radio 0
ap(config-if)# encryption vlan 31 mode ciphers aes-ccm
ap(config-if)# ssid batman
ap(config-if)# end
```

Assigning Names to VLANs

You can assign a name to a VLAN in addition to its numerical ID. VLAN names can contain up to 32 ASCII characters. The access point stores each VLAN name and ID pair in a table.

Guidelines for Using VLAN Names

Keep these guidelines in mind when using VLAN names:

- The mapping of a VLAN name to a VLAN ID is local to each access point, so across your network, you can assign the same VLAN name to a different VLAN ID.

Note If clients on your wireless LAN require seamless roaming, We recommend that you assign the same VLAN name to the same VLAN ID across all access points, or that you use only VLAN IDs without names.

- Every VLAN configured on your access point must have an ID, but VLAN names are optional.
- VLAN names can contain up to 32 ASCII characters. However, a VLAN name cannot be a number between 1 and 4095. For example, *vlan4095* is a valid VLAN name, but *4095* is not. The access point reserves the numbers 1 through 4095 for VLAN IDs.

Creating a VLAN Name

Beginning in privileged EXEC mode, follow these steps to assign a name to a VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 vlan-name** *name* **vlan** *vlan-id*	Assign a VLAN name to a VLAN ID. The name can contain up to 32 ASCII characters.

	Command	Purpose
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to remove the name from the VLAN. Use the **show dot11 vlan-name** privileged EXEC command to list all the VLAN name and ID pairs configured on the access point.

Using a RADIUS Server to Assign Users to VLANs

You can configure your RADIUS authentication server to assign users or groups of users to a specific VLAN when they authenticate to the network.

Note Unicast and multicast cipher suites advertised in WPA or RSN Information Element information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, WPA, WPA2 and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

The VLAN-mapping process consists of these steps:

1. A client device associates to the access point using any SSID configured on the access point.
2. The client begins RADIUS authentication.
3. When the client authenticates successfully, the RADIUS server maps the client to a specific VLAN, regardless of the VLAN mapping defined for the SSID the client is using on the access point. If the server does not return any VLAN attribute for the client, the client is assigned to the VLAN specified by the SSID mapped locally on the access point.

These are the RADIUS user attributes used for vlan-id assignment. Each attribute must have a common tag value between 1 and 31 to identify the grouped relationship.

- IETF 64 (Tunnel Type): Set this attribute to **VLAN**
- IETF 65 (Tunnel Medium Type): Set this attribute to **802**
- IETF 81 (Tunnel Private Group ID): Set this attribute to *vlan-id*

Viewing VLANs Configured on the Access Point

In privileged EXEC mode, use the **show vlan** command to view the VLANs that the access point supports. This is sample output from a **show vlan** command:

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0
Dot11Radio1
GigabitEthernet0

   Protocols Configured:   Address:             Received:        Transmitted:
```

```
        Other                                              0                  995

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Other                                              0                  995

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Other                                              0                  995

   4330 packets, 363704 bytes input
   995 packets, 75675 bytes output

Virtual LAN ID:  31 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.31
Dot11Radio1.31
GigabitEthernet0.31

 This is configured as native Vlan for the following interface(s) :
Dot11Radio0
Dot11Radio1
GigabitEthernet0

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 1                0                 5620

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 1                0                 5620

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 1                0                 5620

   0 packets, 0 bytes input
   5620 packets, 2737560 bytes output

Virtual LAN ID:  34 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.34
GigabitEthernet0.34

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 34               0                   0

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 34               0                   0

   0 packets, 0 bytes input
   0 packets, 0 bytes output

Virtual LAN ID:  35 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   Dot11Radio0.35

   Protocols Configured:   Address:              Received:        Transmitted:

   0 packets, 0 bytes input
   0 packets, 0 bytes output
```

Configuring a Non-native VLAN as a Management VLAN

Usually, the native VLAN will always be the management VLAN.

Consider a case where you wish to change the VLAN bridge group to 1 for a non-native VLAN. In such a case you can use the **command dot11 management vlan** *vlanid* to configure the non-native VLAN as a management VLAN.

Conditions and Prerequisites

- You cannot have a native VLAN if you are using a non-native VLAN as a management VLAN.
- Workgroup Bridge is not supported for this feature.
- When changing the management VLAN, any sessions of telnet, GUI users which are in progress will be become unstable or get disrupted due to the change.

Configuration Steps (CLI)

Step 1 Use the command for setting the non-native VLAN as a management VLAN.

ap(config)# dot11 management vlan *vlanid*

Ensure that you do not have a native VLAN when using this command.

Step 2 Remove the bridge group 1 from main interface or native

ap(config)# interface d0

ap(config-if)# no bridge-group 1

Step 3 Configure the bridge group 1 to the non-native interface

ap(config-if)# interface 0.5

ap(config-if)# encapsulation dot1q *vlanid*

ap(config-if)# bridge-group 1

ap(config-if)# interface bvi1

Step 4 Setup DHCP

ap(config-if)# *ip-address* dhcp

Configuration Steps (GUI)

Step 1 Go to **Services > VLAN**

Step 2 Under the **Assigned VLANs** section, from the **Current VLAN List**, choose the VLAN to be set as management VLAN

Step 3 Check the **Management VLAN (If non-native)** check box.

Steps to Undo the Configuration (CLI)

Step 1 Use the command for removing the non-native VLAN as a management VLAN.

ap(config)# no dot11 management vlan *vlanid*

Step 2 Move the bridge group 1 to the main interface or to another native VLAN

Step 3 Configure another bridge group to the non-native interface

VLAN Configuration Example

This example shows how to use VLANs to manage wireless devices on a college campus. In this example, three levels of access are available through VLANs configured on the wired network:

- Management access—Highest level of access; users can access all internal drives and files, departmental databases, top-level financial information, and other sensitive information. Management users are required to authenticate using Cisco EAP-FAST.
- Faculty access—Medium level of access; users can access school's Intranet and Internet, access internal files, access student databases, and view internal information such as human resources, payroll, and other faculty-related material. Faculty users are required to authenticate using Cisco PEAP.
- Student access—Lowest level of access; users can access school's Intranet and the Internet, obtain class schedules, view grades, make appointments, and perform other student-related activities. Students are allowed to join the network using static WPA2 personal (Pre-shared key).

In this scenario, a minimum of three VLAN connections are required, one for each level of access. Because the access point can handle up to 16 SSIDs, you can use the basic design shown in Table 14-1.

Table 14-1 Access Level SSID and VLAN Assignment

Level of Access	SSID	VLAN ID
Management	manage (not boss)	01
Faculty	teach	02
Student	learn	03

Managers configure their wireless client adapters to use SSID manage, faculty members configure their clients to use SSID teach, and students configure their wireless client adapters to use SSID learn. When these clients associate to the access point, they automatically belong to the correct VLAN.

You would complete these steps to support the VLANs in this example:

1. Configure or confirm the configuration of these VLANs on one of the switches on your LAN.
2. On the access point, assign an SSID to each VLAN.
3. Assign authentication types to each SSID.
4. Configure VLAN 1, the Management VLAN, on both the Ethernet and dot11radio interfaces on the access point. You should make this VLAN the native VLAN.
5. Configure VLANs 2 and 3 on both the Ethernet and dot11radio interfaces on the access point.
6. Configure the client devices.

Table 14-2 shows the commands needed to configure the three VLANs in this example.

Table 14-2 Configuration Commands for VLAN Example

Configuring VLAN 1	Configuring VLAN 2	Configuring VLAN 3
ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid boss** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid teach** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid learn** ap(config-ssid)# **end**
ap **configure terminal** ap(config) **interface FastEthernet0.1** ap(config-subif) **encapsulation dot1Q 1 native** ap(config-subif) **exit**	ap(config) **interface FastEthernet0.2** ap(config-subif) **encapsulation dot1Q 2** ap(config-subif) **bridge-group 2** ap(config-subif) **exit**	ap(config) **interface FastEthernet0.3** ap(config-subif) **encapsulation dot1Q 3** ap(config-subif) **bridge-group 3** ap(config-subif) **exit**
ap(config)#dot11 ssid manage ap(config-ssid)#vlan 1 ap(config-ssid)#authentication open eap eap_methods ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 1 mode ciphers aes-ccm	ap(config)#dot11 ssid teach ap(config-ssid)#vlan 2 ap(config-ssid)#authentication open eap eap_methods ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 2 mode ciphers aes-ccm	ap(config)#dot11 ssid teach ap(config-ssid)#vlan 3 ap(config-ssid)#authentication open ap(config-ssid)#authentication key-management wpa version 2 ap(config-ssid)#wpa-psk ascii 0 Cisco123 ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 3 mode ciphers aes-ccm

Table 14-3 shows the results of the configuration commands in Table 14-2. Use the **show running** command to display the running configuration on the access point.

Table 14-3 Results of Example Configuration Commands

VLAN 1 Interfaces	VLAN 2 Interfaces	VLAN 3 Interfaces
interface Dot11Radio**0**.1 encapsulation dot1Q 1 native no ip route-cache no cdp enable bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled	interface Dot11Radio**0**.2 encapsulation dot1Q 2 no ip route-cache no cdp enable bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding bridge-group 2 spanning-disabled	interface Dot11Radio**0**.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 bridge-group 3 subscriber-loop-control bridge-group 3 block-unknown-source no bridge-group 3 source-learning no bridge-group 3 unicast-flooding bridge-group 3 spanning-disabled
interface gigabitethernet encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled	interface gigabitethernet encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled	interface gigabitethernet encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled

Notice that when you configure a bridge group on the radio interface, these commands are set automatically:

```
bridge-group 2 subscriber-loop-control
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
bridge-group 2 spanning-disabled
```

When you configure a bridge group on the `gigabitethernet` interface, these commands are set automatically:

```
no bridge-group 2 source-learning
bridge-group 2 spanning-disabled
```