



Configuring VLANs

This chapter describes how to configure your access point/bridge to operate with the VLANs set up on your wired LAN. These sections describe how to configure your access point/bridge to support VLANs:

- [Understanding VLANs, page 13-2](#)
- [Configuring VLANs, page 13-4](#)

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 access point/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.

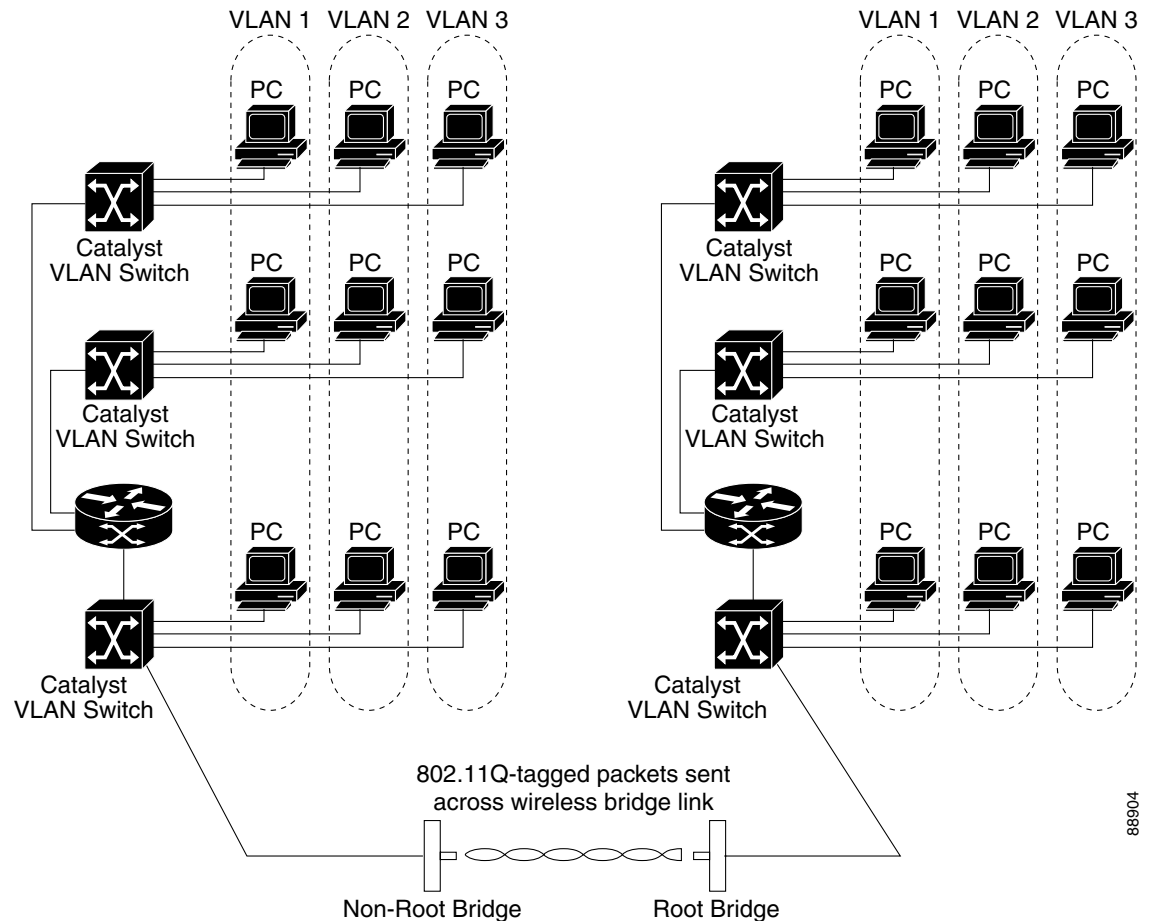
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

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

You extend VLANs into a wireless LAN by adding IEEE 802.11Q tag awareness to the access point/bridge. VLAN 802.1Q trunking is supported between root and non-root access point/bridges through the access point/bridges' primary SSID.

[Figure 13-1](#) shows two access point/bridges sending 802.11Q-tagged packets between two LAN segments that use logical VLAN segmentation.

Figure 13-1 Bridges Connecting LAN Segments Using VLANs



Related Documents

These documents provide more detailed information pertaining to VLAN design and configuration:

- *Cisco IOS Switching Services Configuration Guide*. Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/index.htm
- *Cisco Internetwork Design Guide*. Click this link to browse to this document: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm>
- *Cisco Internetworking Technology Handbook*. Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm
- *Cisco Internetworking Troubleshooting Guide*. Click this link to browse to this document: http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm

Incorporating Wireless Access Point/Bridges into VLANs

The basic wireless components of a VLAN consist of two or more access point/bridges communicating using wireless technology. The access point/bridge is physically connected through a trunk port to the network VLAN switch on which the VLAN is configured. The physical connection to the VLAN switch is through the access point/bridge's Ethernet port.

In fundamental terms, the key to configuring a access point/bridge to connect to a specific VLAN is by configuring its SSID to recognize that VLAN. Since VLANs are identified by a VLAN ID, it follows that if the SSID on a access point/bridge is configured to recognize a specific VLAN ID, a connection to the VLAN is established.

The access point/bridge supports only one SSID. You should assign the SSID to the native VLAN.

Configuring VLANs

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

- [Configuring a VLAN, page 13-4](#)
- [Viewing VLANs Configured on the Access Point/Bridge, page 13-7](#)

Configuring a VLAN

Configuring your access point/bridge to support VLANs is a five-step process:

1. Create subinterfaces on the radio and Ethernet interfaces.
2. Enable 802.1q encapsulation on the subinterfaces and assign one subinterface as the native VLAN.
3. Assign a access point/bridge group to each VLAN.
4. (Optional) Enable WEP on the native VLAN.
5. Assign the access point/bridge's SSID to the native VLAN.

This section describes how to assign an SSID to a VLAN and how to enable a VLAN on the access point/bridge radio and Ethernet ports. For detailed instructions on assigning authentication types to SSIDs, see [Chapter 10, "Configuring Authentication Types."](#)

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio0.x	Create a radio subinterface and enter interface configuration mode for the subinterface.
Step 3	encapsulation dot1q <i>vlan-id</i> [native]	Enable a VLAN on the subinterface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.

	Command	Purpose
Step 4	bridge-group <i>number</i>	Assign the subinterface to a bridge group. You can number your bridge groups from 1 to 255. Note When you enter the bridge-group command, the bridge enables the subinterface to be ready to participate in STP when you enter the bridge n protocol ieee command. See Chapter 8, “Configuring Spanning Tree Protocol,” for complete instructions on enabling STP on the bridge.
Step 5	exit	Return to global configuration mode.
Step 6	interface fastEthernet0.x	Create an Ethernet subinterface and enter interface configuration mode for the subinterface.
Step 7	encapsulation dot1q <i>vlan-id</i> [native]	Enable a VLAN on the subinterface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 8	bridge-group <i>number</i>	Assign the subinterface to a bridge group. You can number your bridge groups from 1 to 255.
Step 9	exit	Return to global configuration mode.
Step 10	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 11	ssid <i>ssid-string</i>	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. You can create only one SSID on the access point/bridge. Note You use the ssid command’s authentication options to configure an authentication type for each SSID. See Chapter 10, “Configuring Authentication Types,” for instructions on configuring authentication types.
Step 12	vlan <i>vlan-id</i>	Assign the SSID to the native VLAN.
Step 13	infrastructure-ssid	Designate the SSID as the infrastructure SSID. It is used to instruct a non-root access point/bridge or workgroup bridge radio to associate with this SSID.

	Command	Purpose
Step 14	encryption [vlan <i>vlan-id</i>] mode wep { optional [key-hash] mandatory [mic] [key-hash]}	(Optional) Enable WEP and WEP features on the native VLAN. <ul style="list-style-type: none"> (Optional) Select the VLAN for which you want to enable WEP and WEP features. Set the WEP level and enable TKIP and MIC. If you enter optional, another access point/bridge can associate to the access point/bridge with or without WEP enabled. You can enable TKIP with WEP set to optional but you cannot enable MIC. If you enter mandatory, other access point/bridges must have WEP enabled to associate to the access point/bridge. You can enable both TKIP and MIC with WEP set to mandatory. <p>Note You can enable encryption for each VLAN, but the access point/bridge uses only the encryption on the native VLAN. For example, if the native VLAN encryption is set to 128-bit static WEP, that is the only encryption method used for traffic between the root and non-root access point/bridge.</p>
Step 15	exit	Return to interface configuration mode for the radio interface.
Step 16	end	Return to privileged EXEC mode.
Step 17	copy running-config startup-config	(Optional) Save your entries in the configuration file.

This example shows how to:

- Enable the VLAN on the radio and Ethernet ports as the native VLAN
- Name an SSID
- Assign the SSID to a VLAN

```
bridge# configure terminal
bridge(config)# interface dot11radio0.1
bridge(config-subif)# encapsulation dot1q 1 native
bridge(config-subif)# bridge group 1
bridge(config-subif)# exit
bridge(config)# interface fastEthernet0.1
bridge(config-subif)# encapsulation dot1q 1 native
bridge(config-subif)# bridge group 1
bridge(config-subif)# exit
bridge(config)# interface dot11radio0
bridge(config-if)# ssid batman
bridge(config-ssid)# vlan 1
bridge(config-ssid)# infrastructure-ssid
bridge(config-ssid)# end
```

Viewing VLANs Configured on the Access Point/Bridge

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

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

    vLAN Trunk Interfaces: Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

    This is configured as native Vlan for the following interface(s) :
Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

    Protocols Configured:  Address:                Received:        Transmitted:
        Bridging           Bridge Group 1      201688           0
        Bridging           Bridge Group 1      201688           0
        Bridging           Bridge Group 1      201688           0

Virtual LAN ID: 2 (IEEE 802.1Q Encapsulation)

    vLAN Trunk Interfaces: Dot11Radio0.2
FastEthernet0.2
Virtual-Dot11Radio0.2

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

