Configuring Access Points in VLANs

This module describes how to configure an access point to operate with the VLANs set up on a wired LAN. This chapter includes the following sections

Understanding VLANs

A VLAN is a switched network that is logically segmented by functions, project teams, or applications, rather than being segmented 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 the workstations and servers of other teams. You use VLANs to reconfigure the network through software rather than by 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 of protocols 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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

You extend VLANs into a wireless LAN by adding IEEE 802.11Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different service set indentifiers (SSIDs) with different Wired Equivalent Privacy (WEP) keys. Only the clients associated with that VLAN receive those packets. Also, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded on to the wired network.

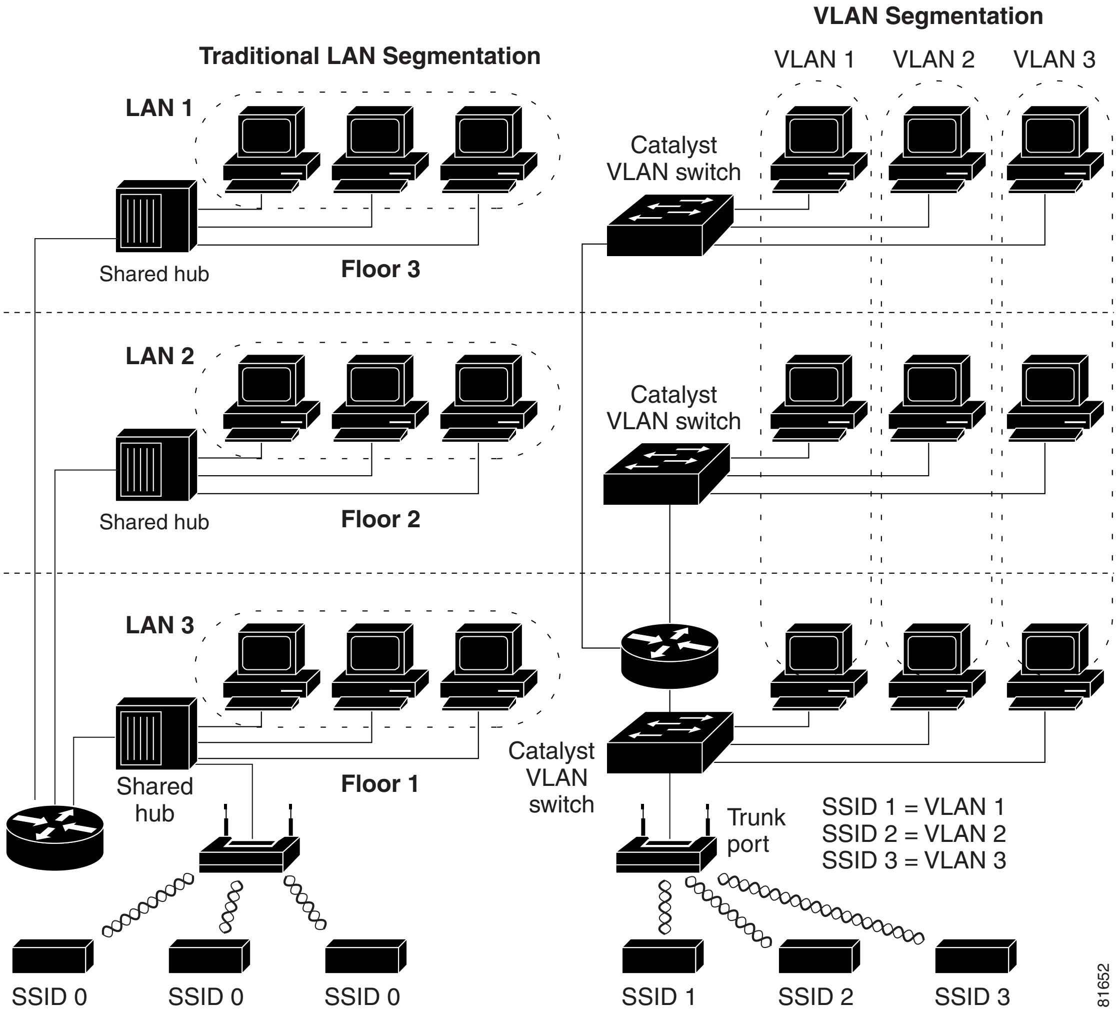
If 802.1q is configured on the Fast Ethernet interface of an access point, the access point always sends keepalives on VLAN 1 even if VLAN 1 is not defined on the access point. As a result, the Ethernet switch connects to the access point and generates a warning message. There is no loss of function on either the access point or the switch. However, the switch log contains meaningless messages that may cause more important messages to be wrapped and not be seen.

Sending these keepalives creates a problem when all SSIDs on an access point are associated to mobility networks. If all SSIDs are associated to mobility networks, the Ethernet switch port that the access point is connected to can be configured as an access port. The access port is normally assigned to the native VLAN of the access point, which is not necessarily VLAN 1, which causes the Ethernet switch to generate warning messages saying that traffic with an 802.1q tag is sent from the access point.

You can eliminate the excessive messages on the switch by disabling the keepalive function.

Figure 1 on page 3 shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 1 LAN and VLAN Segmentation with Wireless Devices



Related Documents

The following documents provide more detailed information about VLAN design and configuration:

- *Cisco IOS Switching Services Configuration Guide.* Click this link to browse to this document: http://cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d129.html
- *Cisco Internetwork Design Guide.* Click this link to browse to this document: http://www.cisco.com/en/US/docs/internetworking/design/guide/idg4.html
- *Cisco Internetworking Technology Handbook.* Click this link to browse to this document: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
- *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 Devices into VLANs

The basic wireless components of a VLAN consist of an access point and a client associated to it through wireless technology. The access point 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 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, if the SSID on an access point is configured to recognize a specific VLAN ID, a connection to the VLAN is established. When this connection is made, associated wireless client devices with 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 an access point, which means that you can support up to 16 VLANs. You can assign only one SSID to a VLAN.

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

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 employees, part-time employees, and guests.
- 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 static WEP, and some wireless users might have more sophisticated devices that use dynamic WEP. You can group and isolate these devices into separate VLANs.

Configuring VLANs

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

Configuring a VLAN

Note When you configure VLANs on access points, the native VLAN must be VLAN 1. In a single architecture, client traffic that is received by the access point is tunneled through an IP-GRE tunnel, which is established on the access point’s Ethernet interface native VLAN. Because of the IP-GRE tunnel, some users may configure another switch port as VLAN1. This misconfiguration causes errors on the switch port.

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

1. Enable the VLAN on the access point radio and Ethernet ports.
2. Assign SSIDs to VLANs.
3. Assign authentication settings to SSIDs.

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 *Authentication Types for Wireless Devices* on Cisco.com, http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html.

For instructions on assigning other settings to SSIDs, see *Service Set Identifiers* on Cisco.com, http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html.

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. Or, the total number VLANs you can configure on your LAN is determined by the number of LANs supported by the host router.

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

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio 0 | 1}**	Enters interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio are 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.

	Command	Purpose
Step 3	**ssid** *ssid-string*	Creates an SSID and enters SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. The first character cannot be any of the following characters: • Exclamation point (!) • Pound sign (#) • Semicolon (;) The following characters are invalid and cannot be used in an SSID: • Plus sign (+) • Right bracket (]) • Front slash (/) • Quotation mark (") • Tab • Trailing spaces You use the **ssid** command authentication options to configure an authentication type for each SSID. See *Using an Access Point as a Local Authenticator* on Cisco.com for instructions on configuring authentication types, http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html
Step 4	**vlan** *vlan-id*	(Optional) Assigns 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 SSID to a VLAN. **Tip** If your network uses VLAN names, you can also assign names to the VLANs on your access point.
Step 5	**exit**	Returns to interface configuration mode for the radio interface.
Step 6	**interface dot11radio [0.x | 1.x]**	Enters interface configuration mode for the radio VLAN subinterface.
Step 7	**encapsulation dot1q** *vlan-id* [**native**]	Enables a VLAN on the radio interface. (Optional) Designates the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 8	**exit**	Returns to global configuration mode.
Step 9	**interface fastEthernet0.x**	Enters interface configuration mode for the Ethernet VLAN subinterface.
Step 10	**encapsulation dot1q** *vlan-id* [**native**]	Enables a VLAN on the Ethernet interface. (Optional) Designates the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 11	**end**	Returns to privileged EXEC mode.
Step 12	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

The following example shows how to:

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

```
ap# configure terminal
ap(config)# interface dot11radio0
ap(config-if)# ssid batman
ap(config-ssid)# vlan 1
ap(config-ssid)# exit
ap(config)# interface dot11radio0.1
ap(config-subif)# encapsulation dot1q 1 native
ap(config-subif)# exit
ap(config)# interface fastEthernet0.1
ap(config-subif)# encapsulation dot1q 1 native
ap(config-subif)# exit
ap(config)# 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. Therefore, 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 that is 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

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

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

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 that are advertised in a WPA 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 cipher suite that is different from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the previous cipher suite. At present, the Wi-Fi Protected Access (WPA) and Cisco Centralized Key Management (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 by using any SSID that is 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 that 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

To view the VLANs that the access point supports, use the **show vlan** command in privileged EXEC mode. 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:
```

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 Light Extensible Authentication Protocol (LEAP).
- Faculty access—Medium level of access. Users can access school intranet and the Internet, access internal files, access student databases, and view internal information such as human resources, payroll, and other faculty-related information. Faculty users are required to authenticate using Cisco LEAP.
- Student access—Lowest level of access. Users can access school 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 WEP.

In this scenario, at least 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 1.

Table 1 Access Level SSID and VLAN Assignment

Level of Access	SSID
Management	boss
Faculty	teach
Student	learn

Managers configure their wireless client adapters to use SSID boss, 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 Fast 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 Fast Ethernet and dot11radio interfaces on the access point.
6. Configure the client devices.

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

Table 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)# **vlan 01** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid teach** ap(config-ssid)# **vlan 02** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid learn** ap(config-ssid)# **vlan 03** 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)# **interface Dot11Radio 0.1** ap(config-subif)# **encapsulation dot1Q 1 native** ap(config-subif)# **exit**	ap(config) **interface Dot11Radio 0.2** ap(config-subif) **encapsulation dot1Q 2** ap(config-subif) **bridge-group 2** ap(config-subif) **exit**	ap(config) **interface Dot11Radio 0.3** ap(config-subif) **encapsulation dot1Q 3** ap(config-subif) **bridge-group 3** ap(config-subif) **exit**

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

Table 3 Results of Example Configuration Commands

VLAN 1 Interfaces	VLAN 2 Interfaces	VLAN 3 Interfaces
interface Dot11Radio0.1 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 Dot11Radio0.2 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 Dot11Radio0.3 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 FastEthernet0.1 encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled	interface FastEthernet0.2 encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled	interface FastEthernet0.3 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 Fast Ethernet interface, these commands are set automatically:

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

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