Configuring Wireless VLANs

This module describes how to configure wireless VLANs on a Cisco 800, 1800, 2800, or 3800 series integrated services router (ISR), hereafter referred to as an access point (AP).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Configuring Wireless VLANs" section on page 122.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Information About Configuring Wireless VLANs

Before you configure VLANs, you should understand the following concepts:

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

VLANs Overview

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.

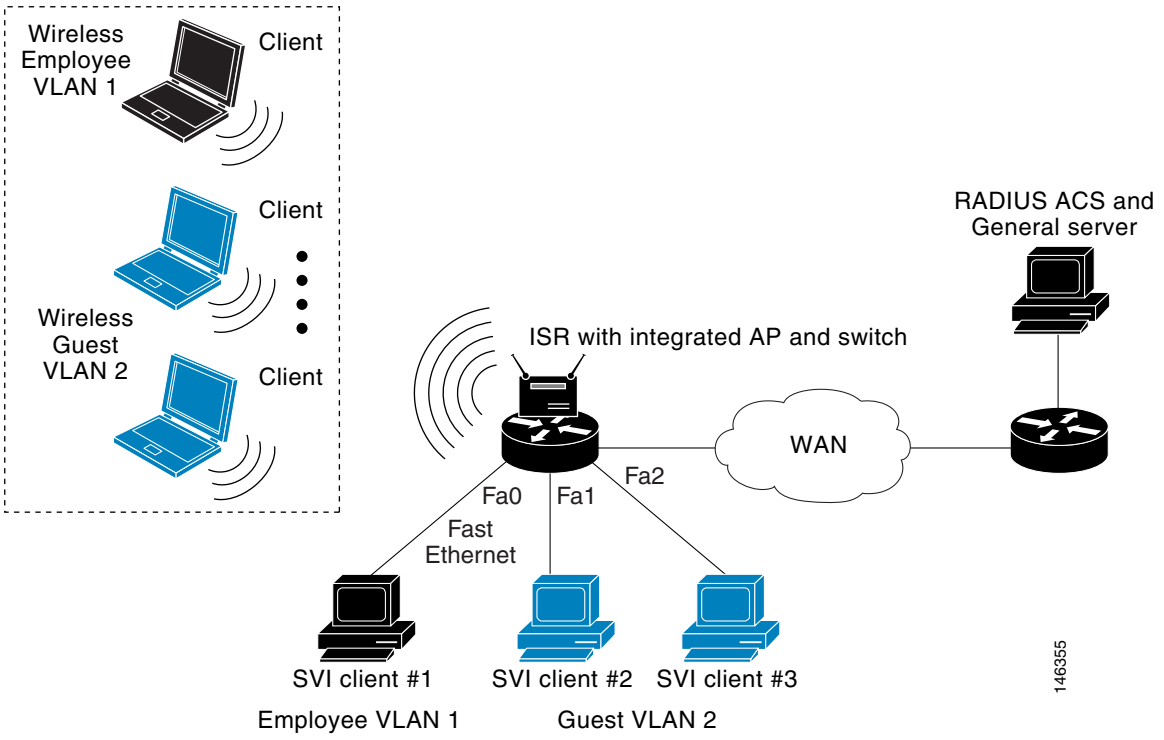
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

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

You extend VLANs into a wireless LAN by adding IEEE 802.11q tag awareness to the AP. Frames destined for different VLANs are transmitted by the AP wirelessly on different Service Set Identifiers (SSIDs). Only the clients associated with that VLAN receive those packets. Each SSID can have one VLAN assigned to it. The benefit of using multiple SSIDs and VLANs is the ability to configure different security features for each group. For example, users in VLAN 1 may be forced to use MAC authentication while users in VLAN 2 do not have that requirement.

Figure 9 shows both wired and wireless VLANs coexisting on a router with an integrated AP and switch.

Figure 9 LAN and VLAN Segmentation with Wireless Devices



Wireless Device Deployment in VLANs

The basic wireless components of a VLAN consist of an AP and a client associated to it using wireless technology.

In fundamental terms, the key to configuring an AP to connect to a specific VLAN is by configuring its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID, it follows that if the SSID on an AP is configured to recognize a specific VLAN ID, 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 AP. 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 10 SSIDs or VLANs on the Cisco 800 series routers, and up to 16 SSIDs or VLANs on the Cisco 1800 series fixed-configuration routers and the Cisco 1841, 2800 and 3800 series modular routers with an AP HWIC. You can assign only one SSID to a VLAN.

The limits for the 16 configurable VLANs on routers with an AP HWIC:

- 1 static and 15 dynamic VLANs
- 1 static and 15 unsecured VLANs
- 16 dynamic VLANs
- 16 unsecured VLANs

The limits for the 16 configurable VLANs on the Cisco 1800 series fixed-configuration routers are:

- 1 static WEP encrypted VLAN, 7 dynamic WEP VLANs, and 8 unsecured VLANs
- 1 static and 15 unsecured VLANs

- 8 dynamic and 8 unsecured VLANs
- 16 unsecured VLANs

The limits for the 10 configurable VLANs on the Cisco 800 series routers are:

- 1 static WEP encrypted VLAN, 3 dynamic WEP VLANs, and 6 unencrypted VLANs

You can use the VLAN feature to deploy wireless devices with greater efficiency and flexibility. For example, one AP can handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple APs 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 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 static WEP, and some wireless users might have more sophisticated devices using dynamic WEP. You can group and isolate these devices into separate VLANs.

Assignment of Users to VLANs Using a RADIUS Server

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

The VLAN-mapping process consists of these steps:

1. A client device associates to the AP using any SSID configured on the AP.
2. The client begins RADIUS authentication.
3. When the client authenticates, 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 AP. 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 AP.

These are the RADIUS user attributes used for VLAN ID assignment. Each attribute must have a common tag value 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 a VLAN ID.

Network Admission Control

Cisco IOS Release 12.4(15)T supports NAC layer 2 (L2) IEEE 802.1x, which extends NAC support to layer 2 switches and wireless access points. Network Admission Control is a Cisco Systems sponsored initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, you can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with an established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.

How to Configure Wireless VLANs

This section contains the following tasks:

- Configuring a Wireless VLAN, page 113 (required)
- Assigning Names to VLANs, page 115 (optional)

Configuring a Wireless VLAN

Using Figure 9 as a reference, perform this task to configure a VLAN on an AP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 ssid** *name*
4. **vlan** *vlan-id*
5. **exit**
6. **interface dot11Radio** *interface*
7. **ssid** *name*
8. **exit**
9. **exit**
10. **interface dot11Radio** *interface.x*
11. **encapsulation dot1q** *vlan-id* [**native**]
12. **end**
13. **copy running-config to startup-config**
14. **show vlans**

15. **show vlans**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dot11 ssid** *name* **Example:** `Router(config)# dot11 ssid anyname`	Creates a global SSID. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length. • The SSID is inactive until you use the **ssid** command in interface configuration mode to assign the SSID to a specific radio interface.
Step 4	**vlan** *vlan-id* **Example:** `Router(config-ssid)# vlan 1`	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.
Step 5	**exit** **Example:** `Router(config-ssid)# exit`	Exits SSID configuration mode and returns to global configuration mode.
Step 6	**interface dot11Radio** *interface* **Example:** `Router(config)# interface dot11Radio 0/3/0`	Enters interface configuration mode for the radio interface. • The *interface* argument is in module/slot/port format, except for the Cisco 800 and Cisco 1800 fixed-configuration series routers, where the *interface* argument is either 0 or 1. • The 2.4-GHz radio port is 0. The 5-GHz radio port is 1.
Step 7	**ssid** *name* **Example:** `Router(config-if)# ssid anyname`	Assigns an SSID to a specific radio interface. • The *name* argument is a case-sensitive alphanumeric string up to 32 characters in length.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-if-ssid)# exit`	Exits SSID configuration mode.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 10	**interface dot11Radio** *interface.x* **Example:** `Router(config)# interface dot11Radio 0/3/0.1`	Enters configuration mode for the Ethernet VLAN subinterface. • On the Cisco 800 and Cisco 1800 fixed-configuration series routers, the *interface* argument is either 0 or 1, which means this command would be entered as **interface dot11Radio 0.1**.
Step 11	**encapsulation dot1q** *vlan-id* [**native**] **Example:** `Router(config-subif)# encapsulation dot1q 1 native`	Sets the encapsulation type for an interface.
Step 12	**end** **Example:** `Router(config-subif)# end`	Returns to privileged EXEC mode.
Step 13	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 14	**show vlans** **Example:** `Router# show vlans`	(Optional) Displays the VLANs that the AP supports.

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

Remember these guidelines 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, Cisco recommends 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 in length. However, a VLAN name cannot be a number from 1 to 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.

Assigning a Name to a VLAN

Perform this task to assign a name to a VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 vlan-name** *name* **vlan** *vlan-id*
4. **end**
5. **copy running-config to startup-config**
6. **show dot11 vlan-name** [*vlan-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dot11 vlan-name** *name* **vlan** *vlan-id* **Example:** `Router(config)# dot11 vlan-name vlan1 vlan 121`	Assigns a name to a VLAN in addition to its numerical ID.
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config** **Example:** `Router# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.
Step 6	**show dot11 vlan-name** [*vlan-name*] **Example:** `Router# show dot11 vlan-name`	(Optional) Displays VLAN names and ID pairs configured on the access point.

Configuration Examples for Wireless VLANs

This section contains the following examples:

- Configuring Wireless VLANs on an Access Point in Bridging Mode: Example, page 118
- Configuring Wireless VLANs on an Access Point in Routing Mode: Example, page 120

VLAN Configuration Scenario

The following VLAN configuration scenario shows how to use VLANs to manage wireless devices in a typical branch office. In this example, two levels of access are available through VLANs configured on the network:

- Employee access—Users can access all company files, databases, and sensitive information. Employees are required to authenticate using Cisco Light Extensible Authentication Protocol (LEAP).
- Guess access—Users can access only the Internet and any external files stored specifically for guest users.

In this scenario, a minimum of two VLAN connections are required, one for each level of access. Because the AP can support up to 16 SSIDs on the AP HWIC and Cisco 1800 fixed-configuration routers, and up to 10 SSIDs on the Cisco 800 series routers, you can use the basic design shown in Table 7.

Table 7 VLAN Basic Design

Level of Access	SSID	VLAN ID
Employee	employee	1
Guest	guest	2

Employees configure their wireless client adapters to use the SSID named employee and guests configure their client adapters to use the SSID named guest. When these clients associate to the AP, they automatically belong to the correct VLAN. Wired clients attached to the router through the integrated switch can also belong to a specific VLAN. Wireless VLAN clients and wired VLAN clients can share subnets or they can belong to completely different subnets. This type of configuration can be accomplished using bridging or integrated routing and bridging (IRB) or routing on the dot11 interface.

The following examples show two configuration methods:

1. Bridge traffic between wireless VLANs and wired VLANs using IRB and route traffic from these networks through the bridged virtual interface (BVI). The clients in the wireless VLANs and wired VLANs will be in the same respective subnets as the IP address of the BVI interfaces.
2. Use routing to keep the wireless and wired VLANs in separate subnets.

Configuring Wireless VLANs on an Access Point in Bridging Mode: Example

Using the VLAN configuration scenario above, perform this task to configure VLAN 1 and VLAN 2 on an AP in bridging mode. When the AP has been configured, configure each client device to recognize either the employee SSID or the guest SSID.

This task includes the following configuration steps:

- Create a global SSID.
- Assign a VLAN to each configured SSID.
- Assign authentication types to each SSID.
- Configure subinterfaces and 802.1q encapsulation for each VLAN under the dot11 interface.
- Assign a bridge group for each subinterface.
- Assign the same bridge group to the relevant wired VLAN.
- Create a BVI interface and assign an IP address for each bridge group.

- Configure the protocol to route each bridge group.

```
configure terminal
 dot11 ssid employee
 vlan 1
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa
 exit
 interface dot11Radio 0/0/0
 no ip address
 encryption vlan 1 mode ciphers aes-ccm
 ssid employee
 exit
 exit
 dot11 ssid guest
 vlan 2
 authentication open
 exit
 interface dot11Radio 0/0/0.1
 encapsulation dot1q 1 native
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 exit
 interface dot11Radio 0/0/0.2
 encapsulation dot1q 2
 bridge-group 2
 exit
 interface FastEthernet 0/1/2
 switchport access vlan 2
 exit
 interface FastEthernet 0/1/3
 switchport access vlan 2
 exit
 interface vlan 1
 bridge group 1
 exit
 interface vlan 2
 bridge group 2
 exit
 interface bvi 1
 ip address 10.10.10.1 255.255.255.0
 exit
 interface bvi 2
 ip address 20.20.20.1 255.255.255.0
 exit
 bridge 1 route ip
 bridge 2 route ip
 exit
 copy running-config to startup-config
```

Configuring Wireless VLANs on an Access Point in Routing Mode: Example

Using the VLAN configuration scenario described in the previous section, perform this task to configure VLAN 1 and VLAN 2 on an AP in routing mode. Routing can be used to keep the wireless and wired VLANs on separate subnets. After the AP has been configured, configure each client device to recognize either the employee SSID or the guest SSID.

This task includes the following configuration steps:

- Create a global SSID.
- Assign a VLAN to each configured SSID.
- Assign authentication types to each SSID.
- Configure subinterfaces and 802.1q encapsulation for each VLAN under the dot11 interface.
- Configure an IP address for each subinterface.

```
configure terminal
 dot11 ssid employee
 vlan 1
 authentication open eap eap_methods
 authentication network-eap eap_methods
 authentication key-management wpa
 exit
 interface dot11Radio 0/0/0
 no ip address
 encryption vlan 1 mode ciphers aes-ccm
 ssid employee
 exit
 exit
 dot11 ssid guest
 vlan 2
 authentication open
 exit
 interface dot11Radio 0/0/0
 ssid guest
 exit
 exit
 interface dot11Radio 0/0/0.1
 encapsulation dot1Q 1 native
 ip address 10.10.10.1 255.255.255.0
 exit
 interface dot11Radio 0/0/0.2
 encapsulation dot1q 2
 ip address 50.50.50.1 255.255.255.0
 end
 copy running-config startup-config
```

Where to Go Next

If you want to configure quality of service (QoS) parameters on an AP, see the “Configuring QoS on an Access Point” module.

Additional References

The following sections provide references related to configuring VLANs for wireless LANs.

Related Documents

Related Topic	Document Title
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Wireless LAN Command Reference*, Release 12.4T
VLAN conceptual information	*Cisco IOS LAN Switching Configuration Guide*, Release 12.4

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	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

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring Wireless VLANs

Table 8 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4T or later appear in the table.

For information on a feature in this technology that is not documented here, see the "Cisco IOS Wireless LAN Features Roadmap" module.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 8 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 8 Feature Information for Configuring Wireless VLANs

Feature Name	Releases	Feature Information
NAC - L2 IEEE 802.1x	12.4(15)T	This feature extends NAC support to layer 2 switches and wireless access points. The following sections provide information about this feature: • Network Admission Control
VLAN Assignment by Name	12.4(15)T	This feature provides the ability for the RADIUS server to assign an 802.1x client to a VLAN identified by name. The following sections provide information about this feature: • Assigning Names to VLANs • Assigning a Name to a VLAN