



Configuring VLANs

This chapter describes VLANs and provides information about configuring them on an access point. The chapter guides you through the process for configuring a typical example VLAN deployment.

This chapter contains the following sections:

- [Entering VLAN Information, page 4-2](#)
- [VLAN Security Policy, page 4-4](#)
- [RADIUS-Based VLAN Access Control, page 4-7](#)
- [Criteria for Deploying Wireless VLANs, page 4-8](#)
- [A Wireless VLAN Deployment Example, page 4-9](#)
- [Guidelines for Wireless VLAN Deployment, page 4-21](#)

Entering VLAN Information

To access the VLAN setup page (see [Figure 4-1](#)), click **VLAN** in the Associations section of the Setup page. You can also access the page from the AP Radio Advanced page in the Network Ports section of the Setup page.

Figure 4-1 VLAN Setup Page

The screenshot shows the 'VLAN Summary Status' page. At the top, there are navigation tabs: Home, Map, Network, Associations, Setup, Logs, and Help. The 'Setup' tab is selected. The page title is 'VLAN Summary Status' and the uptime is '4 days, 00:54:09'. The configuration options are as follows:

- VLAN (802.1Q) Tagging: Enabled Disabled
- 802.1Q Encapsulation Mode: Hybrid Trunk
- Maximum Number of enabled VLAN IDs: 16
- Native VLAN ID:
- Single VLAN ID which allows **Unencrypted** packets: (0=all require encryption)
- Optionally allow **Encrypted** packets on the unencrypted VLAN: yes no

Below these options, there are input fields for 'VLAN ID' and 'VLAN Name', followed by an 'Add New' button. A section titled 'Existing VLANs:' contains a list box with the following items:

- 1 Native VLAN
- 2 Full-Time
- 3 Part-Time
- 4 Guest
- 5 Maintenance
- *When VLAN Disabled*

To the right of the list box are 'Edit' and 'Remove' buttons. At the bottom of the page are 'Apply', 'OK', 'Cancel', and 'RestoreAll' buttons. A small number '61743' is visible in the bottom right corner of the screenshot area.

Follow this link path to reach the VLAN Setup page:

1. On the Summary Status page, click **Setup**. The Setup page appears.
2. In the Associations section, click **VLAN**. The VLAN Setup page appears.

Settings on the VLAN Setup page

The VLAN setup page contains the following settings:

- [VLAN Summary Status Link](#)
- [VLAN \(802.1Q\) Tagging](#)
- [802.1Q Encapsulation Mode](#)
- [Maximum Number of Enabled VLAN IDs](#)
- [Native VLAN ID](#)
- [Single VLAN ID which allows Unencrypted packets](#)
- [Optionally allow Encrypted packets on the unencrypted VLAN](#)

- [VLAN ID](#)
- [VLAN Name](#)
- [Existing VLANs](#)

VLAN Summary Status Link

Clicking this link takes you to a page containing a listing of existing VLANs on the access point. The list provides you with configuration information for each VLAN. [Figure 4-2](#) shows a typical VLAN Summary Status page.

Figure 4-2 VLAN Summary Status Page

| Home | Map | Network | Associations | Setup | Logs | Help | 2002/10/29 14:34:14 | | |
|---|-------------|----------|--------------|----------------|------|-------|-------------------------------------|--------|------------|
| 802.1Q Encapsulation Mode: Hybrid Trunk | | | | | | | VLAN Detailed Setup | | |
| ID | Name | Enabled? | Def. Pri. | Def. Pol. Grp. | MIC | TKIP | Key Rotate | Alert? | Encryption |
| 1(N) | Native VLAN | yes | best effort | [0] | none | Cisco | 0 | no | full |
| 2 | | no | best effort | [0] | none | none | 0 | no | optional |
| 3 | Part-Time | yes | best effort | [0] | none | Cisco | 0 | no | full |
| 4 | Guest | yes | best effort | [0] | none | none | 0 | no | optional |
| 5 | Maintenance | yes | best effort | [0] | none | none | 0 | no | full |
| | | | | | | | | | Done |

86167

VLAN (802.1Q) Tagging

Determines whether the IEEE 802.1Q protocol is used to tag VLAN packets. IEEE 802.1Q protocol is used to connect multiple switches and routers and for defining VLAN topologies. This setting is user configurable.

Early 340 series access points are incompatible with VLAN tagging. Early versions of the 340 series access point can set up VLANs, but clients on non-native VLANs cannot transmit and receive large packets because early 340 series access points were limited to a packet data length of 1500 bytes.

You can identify an affected access point by browsing to the Ethernet Identification page and checking the Maximum Packet Data Length parameter. If it is 1500, the failure will occur.

If you have an early 340 series access point on your network, you can eliminate the problem by setting the Maximum Packet Data Length parameter for all other devices to 1400 bytes.

802.1Q Encapsulation Mode

A status setting that indicates whether or not IEEE 802.1Q tagging is in use. This field always displays **disabled** unless the following conditions are met:

- VLAN (802.1Q) tagging is enabled.
- A valid and enabled VLAN is specified as the native VLAN ID.

Maximum Number of Enabled VLAN IDs

A status setting that provides the maximum number of VLANs that can reside on the access point. This setting is for information only and is not configurable.

Native VLAN ID

Specifies the identification number of the access point's native VLAN. This configurable setting must agree with the native VLAN ID setting on the switch.

Single VLAN ID which allows Unencrypted packets

Identifies the number of the VLAN on which unencrypted packets can pass between the access point and the switch. This setting is configurable.

Optionally allow Encrypted packets on the unencrypted VLAN

Determines whether the access point passes encrypted packets on an unencrypted VLAN. This setting permits a client device to associate to the access point allowing both WEP and non-WEP associations.

VLAN ID

A unique number that identifies a VLAN. This number must match VLANs set on the switch. The setting is configured by the user.

VLAN Name

A unique name for a VLAN configured on the access point. This setting is configured by the user. The VLAN name is for information only and is not used by the switch or access point as a parameter for determining the destination of data.

Existing VLANs

A list of successfully configured VLANs on the access point. As the user configures VLANs, they appear in this list by ID number and name. From this list, you can edit or remove a VLAN.

VLAN Security Policy

You can define a security policy for each VLAN on the access point. This enables you to define the appropriate restrictions for each VLAN you configure. The following parameters can be configured on the wireless SSID page:

- SSID Name—a unique name for each wireless VLAN
- Maximum number of associations—ability to limit maximum number of wireless clients per SSID
- Default VLAN ID—VLAN ID mapping on the wired side
- Policy Group ID—The identification number of the applicable policy group
- Accept Authentication types—Open, Shared, and Network-EAP

- Require EAP: —Under Open, Shared, and Network-EAP
- Default Unicast Address Filter—Allowed or Disallowed under Open, Shared, and Network-EAP
- MAC authentication—Under Open, Shared, and Network-EAP when the Default Unicast Address Filter setting is Disallowed

The following parameters can be configured on the VLAN ID page:

- VLAN Name—The unique name for the VLAN
- VLAN Enable—Enables or disables this VLAN
- Default Priority—Ability to apply default CoS for each VLAN
- Default Policy Group—Ability to apply a policy group (set of Layer 2, 3, and 4 filters) for each VLAN. Each filter within a policy group can be configured to allow or deny a certain type of traffic
- Temporal Key Integrity Protocol (TKIP)—Ability to enable per packet key hashing for each VLAN
- Enhanced MIC verification for WEP—Ability to enable MIC per VLAN
- WEP key rotation interval—Ability to enable WEP key rotation for each VLAN but supported only for wireless VLANs with IEEE 802.1x protocols enabled (such as LEAP, EAP-TLS, PEAP, etc.)
- Encryption key—The key used for broadcast or multicast segmentation per VLAN. This key is also used for static WEP clients for both unicast and multicast traffic



Note

With an encryption key configured, the VLAN supports standardized WEP. However, TKIP, MIC, and broadcast key rotation features can optionally be configured as noted above.

Table 4-1 lists the SSID and VLAN ID configuration parameters.

Table 4-1 SSID and VLAN ID Configuration Parameters

| Parameter | SSID Parameter | VLAN ID Parameter |
|--------------------------------|----------------|-------------------|
| Authentication types | x | |
| Maximum number of associations | x | |
| Encryption key (broadcast key) | | x |
| TKIP/MIC | | x |
| WEP rotation interval | | x |
| Policy group | | x |
| Default Priority (CoS mapping) | | |

Broadcast Domain Segmentation

All Layer 2 broadcast and multicast messages are propagated over the air so that each WLAN client receives broadcast and multicast traffic belonging to different VLANs. A wired client receives Layer 2 broadcast and multicast traffic only for its own VLAN. Therefore, a unique broadcast/multicast encryption key is used to segment the Layer 2 broadcast domains on the wireless LAN. The unique encryption key must be configured during initial VLAN setup. If broadcast key rotation is enabled, this encryption key is generated dynamically and delivered to WLAN clients in IEEE 802.1x messages.

The requirement to segment broadcast domains on the wireless side restricts the use of unencrypted VLAN per ESS. A maximum of one VLAN can be unencrypted per WLAN ESS. The behavior of a WLAN client on an encrypted VLAN should be to discard unencrypted Layer 2 broadcast or multicast traffic.

Native VLAN Configuration

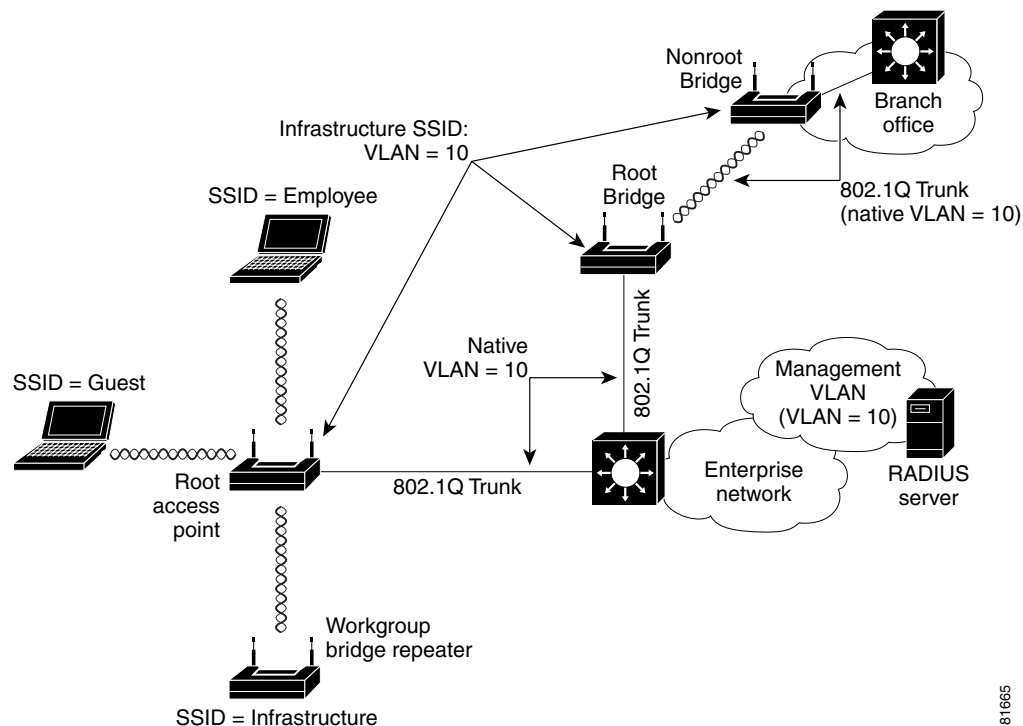
The native VLAN setting on the access point must match the native VLAN of the wired trunk. Also, the access point receives and communicates using the Inter-Access Point Protocol (IAPP) with other access points in the same wireless LAN ESS using the native VLAN. Therefore, it is a requirement that all access points in an ESS must use the same native VLAN ID. Furthermore, all Telnet and http management traffic as well as the RADIUS traffic is routed to the access point through the native VLAN. It is recommended that you restrict user access to the native (default) VLAN of the access points through the use of Layer 3 ACLs and policies on the wired infrastructure side.

You may or may not wish to map the native VLAN of the access point to an SSID (for example, to the wireless ESS). Scenarios where the native VLAN must be mapped to an SSID are as follows:

- An associated workgroup bridge to be treated as an infrastructure device
- For a root bridge to connect to a nonroot bridge

In these scenarios, Cisco recommends that you configure an infrastructure SSID for each access point. [Figure 4-3](#) illustrates combined deployment of infrastructure devices along with noninfrastructure devices in an enterprise LAN. As the figure shows, the native VLAN of the access point is mapped to the infrastructure SSID. WEP encryption along with TKIP (at least per packet key hashing) should be turned on for the infrastructure SSID. Cisco also recommends that you configure a secondary SSID as the infrastructure SSID. The concepts of primary and secondary SSIDs are explained in the next section.

Figure 4-3 Deployment of Infrastructure and Non infrastructure Devices



81665

Primary and Secondary SSIDs

When multiple wireless VLANs are enabled on an access point or bridge, multiple SSIDs are created. Each SSID maps to a default VLAN ID on the wireless side. IEEE 802.11 specifications require that only one SSID be broadcast in the beacons, so you must define a primary SSID to be broadcast in the IEEE 802.11 beacon management frames. All other SSIDs are secondary SSIDs and are not broadcast in the beacon management frames.

If a client or infrastructure device (such as a workgroup bridge) sends a probe request with a secondary SSID, the access point or bridge responds with a probe response with a secondary SSID.

You can map the primary SSID to the VLAN ID on the wired infrastructure in different ways. For example, in an enterprise rollout scenario, the primary SSID could be mapped to the unencrypted VLAN on the wired side to provide guest VLAN access.

RADIUS-Based VLAN Access Control

You may want to impose RADIUS-based VLAN access control. For example, if the WLAN setup is such that all VLANs use IEEE 802.1x and similar authentication mechanisms for WLAN user access, the user can hop from one VLAN to another by changing the SSID and successfully authenticating to the access point. However, this process may not be ideal if the wireless user is to be confined to a particular VLAN.

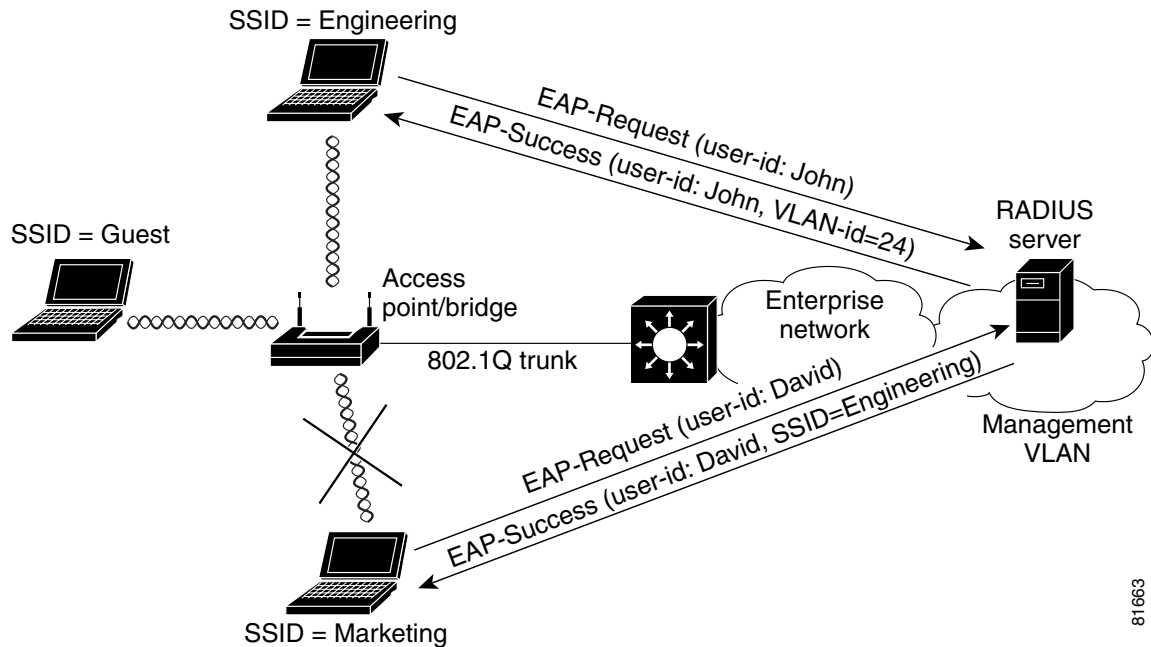
There are two ways to implement RADIUS-based VLAN access control on the access point:

1. RADIUS-based VLAN assignment—upon successful IEEE 802.1x or MAC authentication, the RADIUS server assigns the user to a particular VLAN ID on the wired side. Regardless of which SSID is used for WLAN access, the user is always assigned to a particular VLAN ID.
2. RADIUS-based SSID access control—Upon successful IEEE 802.1x or MAC authentication, the RADIUS server passes back the allowed SSID list and the user is allowed to associate to the WLAN. Otherwise, the user is disassociated from the access point or bridge.

[Figure 4-4](#) illustrates both RADIUS-based VLAN access control methods. In the figure, both Engineering and Marketing VLANs are configured to allow only IEEE 802.1x authentication (LEAP, EAP-TLS, PEAP, etc.). When user John uses the Engineering SSID to access the WLAN, the RADIUS server maps John to VLAN ID 24, which may or may not be the default VLAN ID mapping for the Engineering SSID. Using this method, a user can be mapped to a fixed wired VLAN throughout an enterprise network.

[Figure 4-4](#) also shows an example for RADIUS-based SSID access control. In the figure, David uses the Marketing SSID to access the WLAN however, the permitted SSID list sent back by the RADIUS server allows David to access only the Engineering SSID and the access point disassociates him from the WLAN. Using RADIUS-based SSID access, a user can be given access to one or multiple SSIDs throughout the enterprise network.

Figure 4-4 RADIUS-Based VLAN Access Control



81663

RADIUS user attributes used for VLAN ID assignment are:

- IETF 64 (Tunnel Type)—Set this to VLAN
- IETF 65 (Tunnel Medium Type)—Set this to 802
- IETF 81 (Tunnel Private Group ID)—Set this to VLAN ID

The Cisco IOS/PIX/RADIUS Attribute (009\001 cisco-av-pair) user attribute is used for SSID control. For example, this attribute allows a user to access the WLAN using the Engineering and Marketing SSIDs only.

Criteria for Deploying Wireless VLANs

You should evaluate the need for deploying wireless VLANs in their own environment. Cisco recommends that you review the VLAN deployment rules and policies before considering wireless VLAN deployment and that you use similar policies to extend wired VLANs to the wireless LAN. This section details criteria for wireless VLAN deployment, a summary of rules for wireless LAN (WLAN) VLAN deployment, and best practices to use on the wired infrastructure side when you deploy wireless VLANs.

Criteria for wireless VLAN deployment are likely to be different for each scenario. The following are the most likely criteria:

- Common resources being used by the WLAN:
 - Wired network resources, such as servers, commonly accessed by wireless users
 - QoS level needed by each application (default CoS, voice CoS, etc.)

- Common devices used to access the WLAN, such as the following:
 - Security mechanisms (static WEP, MAC authentication and EAP authentication supported by each device type)
 - Wired network resources, such as servers, commonly accessed by WLAN device groups
 - QoS level needed by each device group
- Revisions to the existing wired VLAN deployment:
 - Existing policies for VLAN access
 - Localized wired VLANs or flat Layer 2 switched network policies
 - Other affected policies

You should consider the following implementation criteria before deploying wireless VLANs:

- Use policy groups (a set of filters) to map wired policies to the wireless side.
- Use IEEE 802.1x to control user access to VLANs by using either RADIUS-based VLAN assignment or RADIUS-based SSID access control.
- Use separate VLANs to implement different classes of service.
- Adhere to any other criteria specific to your organization's network infrastructure.

Based on these criteria, you could choose to deploy wireless VLANs using the following strategies:

- **Segmentation by user groups**—you can segment your WLAN user community and enforce a different security policy for each user group. For example, you could create three wired and wireless VLANs in an enterprise environment for full- and part-time employees, as well as providing guest access.
- **Segmentation by device types**—You can segment your WLAN to enable different devices with different security levels to access the network. For example, you have hand-held devices that support only 40- or 128-bit static WEP coexisting with other devices using IEEE 802.1x with dynamic WEP in the same ESS. Each of these devices would be isolated into separate VLANs.

A Wireless VLAN Deployment Example

This section outlines a typical use of wireless VLANs. For the example, assume your company, XYZ, determines the need for wireless LANs in its network. Following the guidelines in the previous sections, your findings are as follows:

- Five different groups are present at Company XYZ: full-time employees, part-time employees, contract employees, guests, and maintenance workers.
- Full-time and contract employees use company-supplied PCs to access the wireless network. The PCs are capable of supporting IEEE 802.1x authentication methods to access the wireless LAN.
- Full-time employees need full access to the wired network resources. The IT department has implemented application level privileges for each user (using Microsoft NT or 2000 AD mechanisms).
- Part-time and contract employees are not allowed access to certain wired resources (such as HR or data storage servers). The IT department has implemented application level privileges for part time employees (using Microsoft NT or 2000 AD mechanisms).
- Guest users want access to the Internet and are likely to launch a VPN tunnel back to their own company headquarters.

- Maintenance workers use specialized hand-held devices to access information specific to maintenance issues (such as trouble tickets). They access the information from a server in an Application Servers VLAN. The handhelds only support static 40- or 128-bit WEP.
- Existing wired VLANs are localized per building and use Layer-3 policies to prevent users from accessing critical applications.

Using the information above, you could deploy wireless VLANs by creating four wireless VLANs as follows:

- A *full-time* VLAN and a *part-time* VLAN using IEEE 802.1x with dynamic WEP and TKIP features for WLAN access. User login is tied to the RADIUS server with a Microsoft back-end user database. This configuration enables the possibility of single sign-on for WLAN users.
- RADIUS-based SSID access control for both full-time and part-time employee WLAN access. Cisco recommends this approach to prevent part-time employees from VLAN hopping, such as trying to access the WLAN using the full-time VLAN.

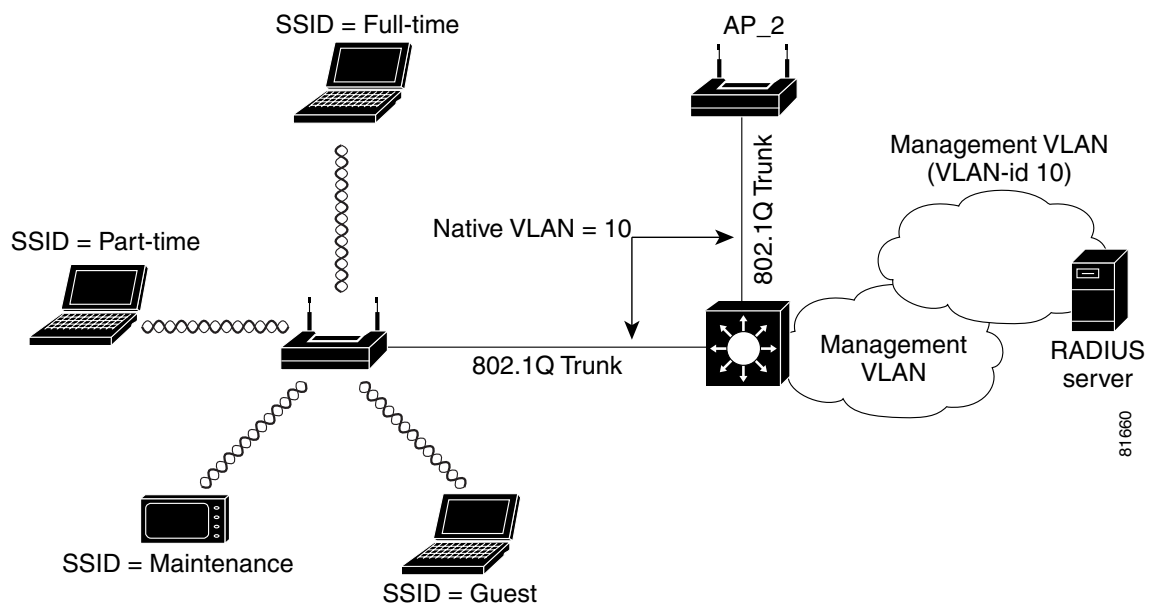


Note In this deployment scenario, VLANs are localized per building, enabling users to access the WLAN from anywhere within the campus. Cisco recommends using SSID access control rather than using fixed VLAN ID assignment.

- A *guest* VLAN uses the primary SSID with open or no WEP access. Policies are enforced on the wired network side to force all guest VLAN access to an Internet gateway and denies access into the XYZ corporate network.
- A *maintenance* VLAN uses open with WEP plus MAC authentication. Policies are enforced on the wired network side to allow access only to the maintenance server on the application server's VLAN.

Figure 4-5 shows the wireless VLAN deployment scenario described above.

Figure 4-5 Wireless VLAN Deployment Example



Using the Configuration Screens

Using the example outlined above, this section describes how to use the configuration screens to configure VLANs on your access point.

To create and enable VLANs on your access point you must complete the following procedures:

1. Obtain and record the VLAN ID and setup information for the switch to which your access point will communicate.
2. Create and configure the VLANs on your access point.
3. Create and configure the SSIDs to which the VLANs will associate.
4. Enable VLAN (802.1Q) tagging.
5. Identify the native VLAN.

Obtaining and Recording VLAN ID and Setup Information

See your organization's network administrator to obtain the information you need to create VLANs on your access point. For this example, [Table 4-2](#) lists the information required to configure the VLANs on the access point.

Table 4-2 Configuration for Example VLAN Deployment

| SSID | VLAN ID | Security Policy |
|---------------------|---------|---|
| Infrastructure VLAN | 1 | IEEE 802.1x with Static WEP + TKIP/MIC |
| Full-time | 2 | IEEE 802.1x with Dynamic WEP + TKIP/MIC |
| Part-time | 3 | IEEE 802.1x with Dynamic WEP + TKIP/MIC |
| Guest | 5 | Open with no WEP |
| Maintenance | 4 | Open with WEP + MAC authentication |

Creating and Configuring VLANs on the Access Point

For this example, you will create 5 VLANs using the information in [Table 3-2](#).



Note

To avoid error messages in the event log, do not enable the VLANs until you have finished creating them and associated SSIDs to them.

Creating the Native VLAN

You must create and identify a native VLAN before the access point can connect to the trunk and communicate with the switch. Follow these steps to create the native VLAN.

- Step 1** Use your web browser to browse to the access point's summary status page.
- Step 2** Click **Setup**. The Setup page appears.
- Step 3** In the Associations section, click **VLAN**. The VLAN Setup page appears (Figure 4-6).

Figure 4-6 VLAN Setup Page

The screenshot shows the 'VLAN Summary Status' page. At the top, there are navigation tabs: Home, Map, Network, Associations, Setup, Logs, and Help. The 'Setup' tab is selected. The page title is 'VLAN Summary Status' and the uptime is '05:50:24'. The configuration options are as follows:

- VLAN (802.1Q) Tagging: Enabled Disabled
- 802.1Q Encapsulation Mode: --Disabled--
- Maximum Number of enabled VLAN IDs: 16
- Native VLAN ID:
- Single VLAN ID which allows **Unencrypted** packets: (0=all require encryption)
- Optionally allow **Encrypted** packets on the unencrypted VLAN: yes no

Below these options, there is a section for 'Existing VLANs:'. It contains a table with one entry: '*When VLAN Disabled*'. To the right of the table are 'Edit' and 'Remove' buttons. At the bottom of the page are 'Apply', 'OK', 'Cancel', and 'RestoreAll' buttons.

- Step 4** Enter 1 in the Default VLAN ID field.
- Step 5** Enter Native VLAN in the VLAN Name field.
- Step 6** Click **Add New**. The VLAN ID #1 Setup Page appears (Figure 4-7).

Figure 4-7 VLAN ID #1 Setup Page

Map Help Uptime: 6 days, 00:35:02

VLAN Name: Native VLAN

VLAN Enable: Enabled Disabled

Default Priority: default

Default Policy Group: [0] None

Enhanced MIC verification for WEP: None

Temporal Key Integrity Protocol: None

WEP Key Rotation Interval: 0 (0=off)

Alert?: yes no

| | Encryption Key | Key Size |
|------------|----------------------------|----------|
| WEP Key 1: | 12345678901234567890123456 | 128 bit |
| WEP Key 2: | | not set |
| WEP Key 3: | | not set |
| WEP Key 4: | | not set |

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).

Apply OK Cancel Restore Defaults

- Step 7** Make the following entries on this page:
- VLAN Name: Native VLAN (should be displayed)
 - VLAN Enable: Enable
 - Default Priority: default
 - Default Policy Group: None
 - Enhanced MIC verification for WEP: None
 - Temporal Key Integrity Protocol: Cisco
 - WEP Key 1: Enter 26 hexadecimal characters.
 - Key Size: 128 bit
- Step 8** Click **OK** to save your settings and return to the VLAN Setup screen.

Creating the Full- and Part-Time VLANs

The full- and part-time VLANs are essentially the same except for their names and SSIDs. Follow these steps to create these VLANs.

-
- Step 1** On the VLAN Setup page, make the following changes:
- VLAN (802.1Q) Tagging: Enabled
 - Native VLAN ID: 0
 - Single VLAN which allows Unencrypted packets: 0
 - Optionally allow Encrypted packets on the unencrypted VLAN: yes
 - VLAN ID: 2
 - VLAN Name: Full-Time
- Step 2** Click **Add New**. The VLAN ID #2 page appears.
- Step 3** Make the following entries on this page:
- VLAN Name: Full-Time
 - VLAN Enable: Enabled
 - Default Priority: default
 - Default policy group: [0] None
 - Enhanced MIC verification for WEP: None
 - Temporal Key Integrity Protocol: Cisco
 - WEP Key Rotation Interval: 0
 - Alert?: no
 - WEP Key 1: Enter 26 hexadecimal characters.
 - Key Size: 128 bit
- Step 4** Click **OK** to save your settings and return to the VLAN Setup page.
- Step 5** Create the Part-Time VLAN using the same settings as Full-Time with the following exceptions:
- VLAN ID: 3
 - VLAN Name: Part-Time
- Step 6** Click **Add New**. The VLAN ID #3 page appears.
- Step 7** Make the same entries for this page as you did for the Full-Time VLAN.
- Step 8** Click **OK** to save your settings and return to the VLAN Setup page.
-

Creating the Guest VLAN

-
- Step 1** Create a “Guest” VLAN using the following configuration:
- VLAN (802.1Q) Tagging: Disabled
 - Native VLAN ID: 0
 - Single VLAN ID which allows Unencrypted packets: 0
 - Optionally allow Encrypted packets on the unencrypted VLAN: yes
 - VLAN ID: 4
 - VLAN Name: Guest
- Step 2** Click **Add New**. The VLAN ID #4 page appears.
- Step 3** Make the following entries on this page:
- VLAN Name: Guest
 - VLAN Enable: Enabled
 - Default Priority: default
 - Default Policy Group: [0] None
 - Enhanced MIC verification for WEP: None
 - Temporal Key Integrity Protocol: None
 - WEP Key Rotation Interval: 0
 - Alert?: no
 - WEP Key (1- 4): No entries required



Note Apply a policy group (set of L2, L3, and L4 filters) for this VLAN.

- Step 4** Click **OK** to save your settings and return to the VLAN Setup page.
- Step 5** On the VLAN Setup page, identify your Guest VLAN (4) in the Single VLAN ID that allows **Unencrypted** packets field and set the Optionally allow **Encrypted** packets on the unencrypted VLAN to **Yes**.
-

Creating the Maintenance VLAN

- Step 6** Add an encrypted VLAN using the following configuration:
- VLAN (802.1Q) Tagging: Disabled
 - Native VLAN ID: 0
 - Single VLAN ID which allows Unencrypted packets: 0
 - Optionally allow Encrypted packets on the unencrypted VLAN: no
 - VLAN ID: 5
 - VLAN Name: Maintenance
- Step 7** Click **Add New**. The VLAN ID #5 page appears.

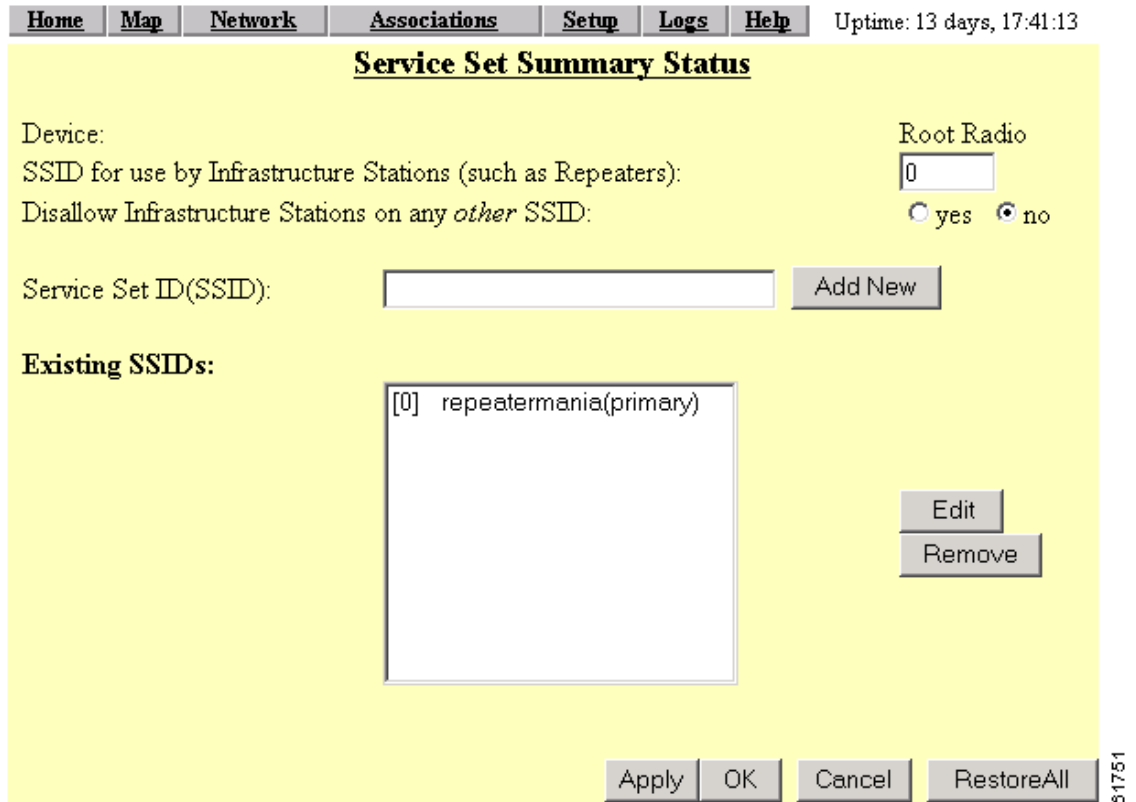
- Step 8** Make the following entries on this page:
- a. VLAN Name: Maintenance
 - b. VLAN Enable: Enabled
 - c. Default Priority: default
 - d. Default policy group: [0] None
 - e. Enhanced MIC verification for WEP: None
 - f. Temporal Key Integrity Protocol: None
 - g. WEP Key Rotation Interval: 0
 - h. Alert?: no
 - i. WEP Key 1: Set a 128-bit key.
- Step 9** Click **OK** to return to the VLAN Setup page.
- Step 10** Verify that your VLANs are listed in the Existing VLANs field.
-

Creating and Configuring the SSIDs

After you create the VLANs for your access point, you create the SSIDs to which the VLANs associate. Follow these steps to create the SSIDs.

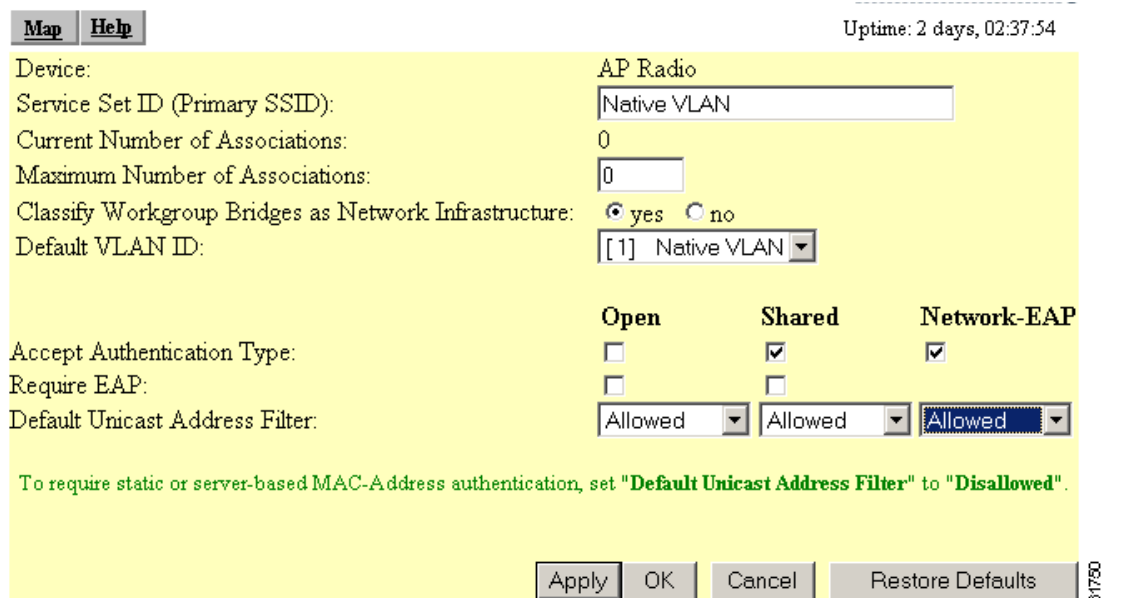
-
- Step 1** Click **Setup** to return to the Setup page.
- Step 2** Click **Service Sets**. The AP Radio Service Sets page appears ([Figure 4-8](#)).

Figure 4-8 AP Radio Service Sets Page



Step 3 In the Existing SSIDs field, highlight the SSID and click **Edit**. The AP Radio Primary SSID page appears (Figure 4-9).

Figure 4-9 AP Radio Primary SSID Page



- Step 4** Make the following changes to this page:
- a. Rename the Primary SSID to Guest VLAN.
 - b. Maximum under of Associations: 0
 - c. Default VLAN ID: [1] Native VLAN.



Note Associating the Default VLAN ID to the native VLAN field is known as mapping the VLAN to the SSID. The mapping process is how the access point is able to “connect” to the VLAN on the switch.

- d. Classify Workgroup Bridges as Network Infrastructure: yes
 - e. Accept Authentication Type: Shared and Network EAP
 - f. Default Unicast Address Filter: Allowed for each authentication type.
- Step 5** Click **OK**. The AP Radio Service Sets page appears.
- Step 6** In the Service Set ID (SSID) field, enter **full-time** and click **Add New**. The AP Radio SSID #1 page appears (Figure 4-11).
- Step 7** Map the full-time SSID to the full-time VLAN ID by following these steps:
- a. Highlight the full-time SSID.
 - b. In the VLAN ID drop-down menu, select [2] **full-time** VLAN ID.
- Step 8** Select Network-EAP authentication type and allow default unicast address filters.
- Step 9** Click **OK** to save your settings and return to the AP Radio Service Sets page.
- Step 10** In the Service Set ID (SSID) field, enter Part-Time and click **Add New**. The AP Radio SSID #2 page appears.
- Step 11** Map the Part-Time SSID to the [3] Part-Time VLAN ID.
- Step 12** Select Network-EAP authentication type and allow default unicast address filters.
- Step 13** Click **OK** to save your settings and return to the AP Radio Service Sets page.
- Step 14** Create the Guest SSID and map it to the [4] Guest Default VLAN ID.
- Step 15** Select Open authentication type and allow default unicast address filters.
- Step 16** Click **OK** to save your settings and return to the AP Radio Service Sets page.
- Step 17** Create the Maintenance SSID and map it to the [5] Maintenance Default VLAN ID.
- Step 18** Select Open authentication type and Disallow default unicast address filters.



Note Selecting **Disallow** in this field allows the maintenance hand-held devices to use MAC authentication.

- Step 19** Click **OK** to save your settings and return to the AP Radio Service Sets page.
-

Enabling VLAN (802.1Q) Tagging and Identifying the Native VLAN

When you have finished creating and configuring the VLANs and their associated SSIDs, you must enable VLAN IEEE 802.1Q tagging to make them operational. You must also identify the native VLAN. Follow these steps to enable VLAN IEEE 802.1Q tagging and identify the native VLAN.

- Step 1** Browse to the Summary Status page and click **VLAN** in the Associations section. The VLAN Setup page appears (Figure 4-10).

Figure 4-10 VLAN Setup Page

Home Map Network Associations Setup Logs Help Uptime: 2 days, 21:31:29

VLAN (802.1Q) Tagging: Enabled Disabled

802.1Q Encapsulation Mode: --Disabled--

Maximum Number of enabled VLAN IDs: 16

Native VLAN ID:

Single VLAN ID which allows **Unencrypted** packets: (0=all require encryption)

Optionally allow **Encrypted** packets on the unencrypted VLAN: yes no

VLAN ID: VLAN Name:

Existing VLANs:

| | |
|----------------------|-------------|
| 1 | Native VLAN |
| 2 | Full-Time |
| 3 | Part-Time |
| 4 | Guest |
| 5 | Maintenance |
| *When VLAN Disabled* | |

61762

- Step 2** Verify that the VLANs you created appear in the Existing VLANs field.
- Step 3** Click **Cancel** to return to the Setup page.
- Step 4** Click **Service Sets**. The AP Radio Service Sets page appears (Figure 4-11).

Figure 4-11 AP Radio Service Sets Page

Home Map Network Associations Setup Logs Help Uptime: 2 days, 21:36:35

Device: AP Radio

SSID for use by Infrastructure Stations (such as Repeaters): 0

Disallow Infrastructure Stations on any other SSID: yes no

Service Set ID(SSID): Add New

Existing SSIDs:

- [0] Native VLAN(primary)
- [1] Full-Time
- [2] Part-Time
- [3] Guest
- [4] Maintenance

Edit Remove

Apply OK Cancel RestoreAll 61759

- Step 5** Verify that the SSIDs you created appear in the Existing SSIDs field.
- Step 6** If the VLANs and SSIDs verified in Steps 2 and 5 are correct, go to Step 7. If not, review the procedures and correct the problem.
- Step 7** In the VLAN (802.1Q) field, click **Enable**.
- Step 8** In the Native VLAN ID field, enter 1.
- Step 9** Click **OK**. The 802.1Q Encapsulation Mode setting changes from Disabled to Hybrid Trunk.

Your wireless network is ready to operate using the VLANs you have created.

Creating an SSID for Infrastructure Devices

You must map the native VLAN to an SSID for infrastructure devices (such as workgroup bridges and repeaters) so that they can communicate in the VLAN environment. Follow these steps.

-
- Step 1** From the Setup page, click **Service Sets**.
- Step 2** Create a new SSID called *Infrastructure* and map it to the Native VLAN.
- Step 3** Return to the AP Radio Service Sets page. Highlight the Infrastructure SSID in the Existing SSIDs field.
- Step 4** In the Disallow Infrastructure Stations on any *other* SSID field, click **Yes**.
-

Guidelines for Wireless VLAN Deployment

You may want to consider these guidelines before you deploy wireless VLANs on your network:

- The switch must be capable of providing an IEEE 802.1Q trunk between it and the access point.
- A maximum of 16 VLANs per ESS are supported; each wireless VLAN is represented with a unique SSID.
- Each VLAN must be configured with a unique encryption key.
- Only one unencrypted VLAN per ESS is permitted.
- Only one primary SSID per ESS is supported.
- TKIP/MIC/Broadcast key rotation can be enabled for each VLAN.
- Open, Shared-Key, MAC, Network-EAP (LEAP), and EAP configuration types can be configured on each SSID.
- Shared-Key authentication is supported only on the SSID mapped to the native VLAN (this is most likely to be the Infrastructure SSID).
- A unique policy group (a set of Layer 2, Layer 3, and Layer 4 filters) is allowed for each VLAN.
- Each SSID is mapped to a default wired VLAN with an ability to override its SSID to VLAN ID using RADIUS-based VLAN access control mechanisms.
- RADIUS-based VLAN ID assignment per user is supported.
- RADIUS-based SSID access control per user is supported.
- Assigning a CoS mapping per VLAN is permitted (8 priority levels are supported).
- The number of clients per SSID is controllable.
- All access points and bridges in the same ESS must use the same native VLAN ID in order to facilitate IAPP communication between them.

Wireless LAN security policies can be mapped to the wired LAN switches and routers.

