CHAPTER

*Figure 1-4 Access Points as Root and Non-root Bridges with Clients*

# Workgroup Bridge

You can configure access points as workgroup bridges. In workgroup bridge mode, the unit associates to another access point as a client and provides a

*Figure 2-2 Express Setup Page*

**Step 3**

*Figure 2-8 Certificate Import Wizard*

**Step 17** Click

Table 2-2 shows an example help location and Help Root URL for an 1100 series access point.

**Step 5** Click **Apply**.

# Disabling the Web-Browser Interface

To prevent all use of the web-browser interface, select the **Disable Web-Based Management** check box on the Services: HTTP-Web Server page and click **Apply**.

# Using Editing Features

This section describes the editing features that can help you manipulate the command line. It contains these sections:



## Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
ap# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# editing
```

T t h

CHAPTER

## Express Security Types

Table 4-2 describes the four security types that you can assign to an SSID.

The following modes are supported

- Root
- Root bridge
- Non Root bridge
- Repeater
-

CHAPTER 5

**Step 3** **end**

This example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
AP(config)# enable password l1u2c3k4y5
```

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level**

To disable username authentication for a specific user, use the **no username** *name* global configuration command.

To disable password checking and allow connections without a password, use the **no login** line configuration command.

### Network Configuration

To configure an access point using the network config

# Understanding Simple Network Time Protocol

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

CHAPTER

# Dynamic Frequency Selection

Access points with 5-GHz radios configured at the factory for use in the United States, Europe,

*Figure 6-2 Basic LBS Network Configur*

The access points thige fohe vcinity. If I4wo access

```
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30 speed 12.0
```

Use the **no**

Use the **no** form of the command to reset the RTS settings to defaults.

# Viewing Voice Reports

You can use a browser to access voice reports listing VoWLAN metrics stored on a WLSE. You can view reports for access point groups and for individual access points.

To view voice reports, follow these steps:

CHAPTER

```
    authentication open
    authentication network-eap eap_methods
!
dot11 ssid mktg
    vlan mktg-normal backup mktg-infected1, mktg-infected2, mktg-infected3
    authentication open
    authentication network-eap eap_methods
!
interface Dot11Radio0
!
encryptiokt-normalkey9 1o
encryptiokt-normalmode ic
!
encryptiokt
encryptiokt
!
 ssd8Tngg!
!
 ssd8 mktg
!

atio-rc!interfaceation open

ation open vgrt18 1 sourge-learnvgrt18 1 unicast-flood!interfaceation open

vgrt18 102 sourge-learng 8. 542cvgrt18 102 unicast-floodeg 8. 5ion open
!iFastEn ation open ne transmit-key vgrt18 1 unicast-flood!encryptioktne trann0 2kt
```

The access point/bridge maintains a separate spanning-tree instance for each active VLAN configured

BPDUs contain information about the sending acce

CHAPTER

Each time the access point tries to use the main servers while they are down, the client device trying to authenticate might report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point tries the local authenticator. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

To remove the local authenticator from the access point configuration, use the **no radius-server host *hostname | ip-address*** global configuration command.

# Configuring EAP-FAST Settings

The default settings for EAP-FAST authentication are suitable for most wireless LANs. However, you can customize the credential timeout values, authority ID, and server keys to match your network requirements.

## Configuring PAC Settings

This section describes how to configure Protected Access Credential (PAC) settings. The first time that

To support the security combinations in Table 11-1, your Cisco Aironet access points and Cisco Aironet client devices must run the following software and firmware versions:

-

CHAPTER

*Figure 12-136*

**Step 3** In the AAA Client Hostname field, enter the name of the WDS device.

**Step 4**

CHAPTER 13

# Configuring RADIUS and TACACS+ Servers

This chapter describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), that provides detailed accounting information

QoS on the wireless LAN focuses on downstream prioritization from the access point. Figure 15-1 shows

CHAPTER

## ACL Logging

CHAPTER 18

# Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between

Table 18-1 lists the SNMP versions and security levels supported on access points.

For detailed information on SNMPv3, click this link to browse to the

CHAPTER 19

# Configuring Repeater and Standby Access Points and Workgroup Bridge Mode

This chapter describes how to configure your access point as a repeater, as a hot standby unit, or as a workgroup bridge. This chapter co

Use the

In the upstream direction, WGB removes the 802.1q header from the packet while sending to the WLC. In the downstream direction while forwarding the packet to the switch connecting the wired-client, the WLC sends the packet to WGB without the 802.1q tag and WGB adds a 4-byte 802.1q header based on the destination mac-address. (For detailed information on VLANs, refer to Chapter 14, “Configuring

# Enabling VideoStream Support on Workgroup Bridges

VideoStream improves the reliability of an IP multicast stream by converting the multicast frame, over the air, to a unicast frame. Cisco IOS Releases 15.2(2)JA and later provide VideoStream support for wired devices connected to workgroup bridges. For access points running release 15.2(2)JA and later, the workgroup bridge is added to the wireless LAN controller (WLC) multicast table, and the workgroup bridge converts the VideoStream unicast frame into

CHAPTER

- The access point forms a password named *username@apname.domain*. The variable

```
ap1.company.com ap1
```

For more information, refer to th

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the access point to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip rcmd remote-usernamemote-user**

CHAPTER

# Checking the Top Panel Indicators

# Indicators on 1300 Outdoor Access Point/Bridges

If your access point/bridge is not associating with a remote bridge or access point, check the four LEDs on the back panel. You can use them to quickly assess the unit's status. For information on using the LEDs during the installation and alignment of the access point/bridge antenna, refer to the *Cisco Aironet*

**Error Message**

# WDS Messages

**Error Message** `WLCCP-WDS-6-REPEATER_STOP: WLCCP WDS on Repeater unsupported, WDS is disabled.`

**Explanation** Repeater access points do not support WDS.

**Recommended Action** None.

**Error Message**