Configuring WLANs

This chapter describes how to configure up to 512 WLANs for your Cisco UWN solution. It contains these sections:

- WLAN Overview, page 7-1
- Configuring WLANs, page 7-2

WLAN Overview

The Cisco UWN solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID. All controllers publish up to 16 WLANs to each connected access point, but you can create up to 512 WLANs and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

Note

Cisco 2106, 2112, 2125, 2500, 2504 Series Controllers, and Cisco Wireless Controller on Cisco Services-Ready Engine (SRE) (WLCM2) support only up to 16 WLANs.

Note

All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

You can associate up to 16 WLANs with each access point group and assign specific access points to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group. See the “Creating Access Point Groups” section on page 7-58 for more information on access point groups.

Note

Controller software releases prior to 5.2 support up to only 16 WLANs. Cisco does not support downgrading the controller from software release 5.2 or later releases to a previous release because inconsistencies might occur for WLANs and wired guest LANs. As a result, you would need to reconfigure your WLAN, mobility anchor, and wired LAN configurations.
We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.

## Configuring WLANs

These sections describe how to configure WLANs:

- Creating WLANs, page 7-2
- Using the GUI to Search WLANs, page 7-7
- Configuring DHCP, page 7-10
- Configuring MAC Filtering for WLANs, page 7-17
- Assigning WLANs to Interfaces, page 7-18
- Configuring the DTIM Period, page 7-19
- Configuring Peer-to-Peer Blocking, page 7-21
- Configuring Layer 2 Security, page 7-24
- Configuring a Session Timeout, page 7-31
- Configuring Layer 3 Security, page 7-33
- Assigning a QoS Profile to a WLAN, page 7-38
- Configuring QoS Enhanced BSS, page 7-40
- Configuring Media Session Snooping and Reporting, page 7-43
- Configuring IPv6 Bridging, page 7-50
- Configuring Cisco Client Extensions, page 7-53
- Configuring Access Point Groups, page 7-56
- Configuring Web Redirect with 802.1X Authentication, page 7-63
- Using the GUI to Disable the Accounting Servers per WLAN, page 7-67
- Disabling Coverage Hole Detection per WLAN, page 7-68
- Configuring NAC Out-of-Band Integration, page 7-69
- Configuring Passive Client, page 7-75

## Creating WLANs

This section describes how to create up to 512 WLANs using either the controller GUI or CLI.

You can configure WLANs with different Service Set Identifiers (SSIDs) or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access.

The controller uses different attributes to differentiate between WLANs with the same SSID.

- WLANS with the same SSID and same L2 Policy cannot be created if the WLAN ID < 17.
- Two WLANS with ids greater than 17 having the same SSID and same L2 policy is allowed provided WLANS are added in different AP groups.
Chapter 7 Configuring WLANs

When creating a WLAN with the same SSID, follow these guidelines and requirements:

- You must create a unique profile name for each WLAN.
- When multiple WLANs with the same SSID get assigned to the same AP radio, you must have a unique Layer 2 security policy so that clients can safely select between them.

WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe responses. The available Layer 2 security policies are as follows:

- None (open WLAN)
- Static WEP or 802.1X
- CKIP
- WPA/WPA2

Although WPA and WPA2 cannot be used by multiple WLANs with the same SSID, you can configure two WLANs with the same SSID with WPA/TKIP with PSK and WPA (Wi-Fi Protected Access)/TKIP (Temporal Key Integrity Protocol) with 802.1X, respectively, or with WPA/TKIP with 802.1X or WPA/AES with 802.1X, respectively.

Some clients might not be able to connect to WLANs properly if they detect the same SSID with multiple security policies. Use this feature with care.

The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP Group. If the 600 Series OEAP is in the default group, the WLAN or remote LAN IDs must be lower than 8.

Cisco Flex 7500 Series Controller does not support the 802.1x security variants on a centrally switched WLAN. For example, the following configurations are not allowed on a centrally switched WLAN:

- WPA1/WPA2 with 802.1x AKM
- WPA1/WPA2 with CCKM
- Dynamic-WEP
- Conditional webauth
- Splash WEB page redirect
If you want to configure your WLAN in any of the above combinations, the WLAN must be configured to use local switching.

Using the GUI to Create WLANs

To create WLANs using the controller GUI, follow these steps:

**Step 1** Choose **WLANs** to open the WLANs page (see Figure 7-1).

**Figure 7-1 WLANs Page**

This page lists all of the WLANs currently configured on the controller. For each WLAN, you can see its WLAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs appears in the upper right-hand corner of the page. If the list of WLANs spans multiple pages, you can access these pages by clicking the page number links.

**Note** If you want to delete a WLAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or select the check box to the left of the WLAN, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the WLAN is removed from any access point group to which it is assigned and from the access point’s radio.

**Step 2** Create a new WLAN by choosing **Create New** from the drop-down list and clicking **Go**. The WLANs > New page appears (see Figure 7-2).
When you upgrade to controller software release 5.2 or later releases, the controller creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it nor delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

**Step 3**  
From the Type drop-down list, choose **WLAN** to create a WLAN.

**Note**  
If you want to create a guest LAN for wired guest users, choose **Guest LAN** and follow the instructions in the “Configuring Wired Guest Access” section on page 11-27.

**Step 4**  
In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN. The profile name must be unique.

**Step 5**  
In the WLAN SSID text box, enter up to 32 alphanumeric characters for the SSID to be assigned to this WLAN.

**Step 6**  
From the WLAN ID drop-down list, choose the ID number for this WLAN.

**Note**  
If the Cisco OEAP 600 is in the default group, the WLAN/Remote LAN IDs need to be set as lower than ID 8.

**Step 7**  
Click **Apply** to commit your changes. The WLANs > Edit page appears (see Figure 7-3).

**Note**  
You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.
Step 8 Use the parameters on the General, Security, QoS, and Advanced tabs to configure this WLAN. See the sections in the rest of this chapter for instructions on configuring specific features for WLANs.

Step 9 On the General tab, select the Status check box to enable this WLAN. Be sure to leave it unselected until you have finished making configuration changes to the WLAN.

Note You can also enable or disable WLANs from the WLANs page by selecting the check boxes to the left of the WLANs that you want to enable or disable, choosing Enable Selected or Disable Selected from the drop-down list, and clicking Go.

Step 10 Click Apply to commit your changes.

Step 11 Click Save Configuration to save your changes.

Using the CLI to Create WLANs

Use these commands to create WLANs using the controller CLI:

- View the list of existing WLANs and to see whether they are enabled or disabled by entering this command:
  
  `show wlan summary`

- Create a new WLAN by entering this command:
  
  `config wlan create wlan_id [profile_name] foreign_ap ssid`

  Note If you do not specify an ssid, the profile_name parameter is used for both the profile name and the SSID.
Chapter 7  Configuring WLANs

Cisco Wireless LAN Controller Configuration Guide

OL-21524-02

Configuring WLANs

Note  When WLAN 1 is created in the configuration wizard, it is created in enabled mode. Disable it until you have finished configuring it. When you create a new WLAN using the `config wlan create` command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

Note  If you want to create a guest LAN for wired guest users, follow the instructions in the “Configuring Wired Guest Access” section on page 11-27.

- Disable a WLAN (for example, before making any modifications to a WLAN) by entering this command:
  
  `config wlan disable {wlan_id | foreign_ap | all}`

  where

  - `wlan_id` is a WLAN ID between 1 and 512.
  - `foreign_ap` is a third-party access point.
  - `all` is all WLANs.

Note  If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

- Enable a WLAN (for example, after you have finished making configuration changes to the WLAN) by entering this command:
  
  `config wlan enable {wlan_id | foreign_ap | all}`

Note  If the command fails, an error message appears (for example, “Request failed for wlan 10 - Static WEP key size does not match 802.1X WEP key size”).

- Delete a WLAN by entering this command:
  
  `config wlan delete {wlan_id | foreign_ap}`

Note  An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point’s radio.

Using the GUI to Search WLANs

You can search for specific WLANs in the list of up to 512 WLANs on the WLANs page. This feature is especially useful if your WLANs span multiple pages, preventing you from viewing them all at once.

To search for WLANs using the controller GUI, follow these steps:
Configuring WLANs

Step 1 On the WLANs page, click **Change Filter**. The Search WLANs dialog box appears (see Figure 7-4).

![Figure 7-4  Search WLANs Dialog Box](image)

Step 2 Perform one of the following:
- To search for WLANs based on profile name, select the **Profile Name** check box and enter the desired profile name in the edit box.
- To search for WLANs based on SSID, select the **SSID** check box and enter the desired SSID in the edit box.
- To search for WLANs based on their status, select the **Status** check box and choose **Enabled** or **Disabled** from the drop-down list.

Step 3 Click **Find**. Only the WLANs that match your search criteria appear on the WLANs page, and the Current Filter field at the top of the page specifies the search criteria used to generate the list (for example, None, Profile Name:user1, SSID:test1, Status: disabled).

**Note** To clear any configured search criteria and display the entire list of WLANs, click **Clear Filter**.

Configuring the Maximum Number of Clients per WLAN

You can set a limit to the number of clients that can connect to a WLAN, which is useful in scenarios where you have a limited number of clients that can connect to a controller. For example, consider a scenario where the controller can serve up to 256 clients on a WLAN and these clients can be shared between enterprise users (employees) and guest users. You can set a limit on the number of guest clients that can access a given WLAN. The number of clients that you can configure per WLAN depends on the platform that you are using.

**Note** The maximum number of clients per WLAN feature is not supported when you use hybrid REAP local authentication.

**Note** The maximum number of clients per WLAN feature is supported only for access points that are in connected mode.

*Table 7-1* describes the number of clients that you can configure for a given platform.
Using the GUI to Configure the Maximum Number of Clients per WLAN

To configure the maximum number of clients per WLAN using the controller GUI, follow these steps:

Step 1  Choose WLANs to open the WLANs page.
Step 2  Click the ID number of the WLAN for which you want to limit the number of clients. The WLANs > Edit page appears.
Step 3  On the Advanced tab, enter the Maximum Allowed Clients text box.
See Table 7-1 for the maximum number of clients supported per platform.
Step 4  Click Apply to commit your changes.

Using the CLI to Configure the Maximum Number of Clients per WLAN

To configure the maximum number of clients per WLAN using the controller CLI, follow these steps:

Step 1  Determine the WLAN ID for which you want to configure the maximum clients by entering this command:

```bash
show wlan summary
```
Obtain the WLAN ID from the list.

Step 2  Configure the maximum number of clients per WLAN by entering this command:

```bash
config wlan max-associated-clients max-clients wlanid
```
Configuring DHCP

WLANs can be configured to use the same or different Dynamic Host Configuration Protocol (DHCP) servers or no DHCP server. Two types of DHCP servers are available: internal and external.

Internal DHCP Server

The controllers contain an internal DHCP server. This server is typically used in branch offices that do not already have a DHCP server. The wireless network generally contains 10 access points or fewer, with the access points on the same IP subnet as the controller. The internal server provides DHCP addresses to wireless clients, direct-connect access points, appliance-mode access points on the management interface, and DHCP requests that are relayed from access points. Only lightweight access points are supported. When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

DHCP option 43 is not supported on the internal server. Therefore, the access point must use an alternative method to locate the management interface IP address of the controller, such as local subnet broadcast, DNS, priming, or over-the-air discovery.

Note

The controller internal DHCP server does not support Aironet 600 Series OfficeExtend Access Point.

Note

See Chapter 8, “Controlling Lightweight Access Points,” or the Controller Deployment Guide at this URL for more information on how access points find controllers:

Note

An internal DHCP server pool will only serve the wireless clients of that controller, not clients of other controllers. Also, internal DHCP server can only serve wireless clients and not wired clients.

Note

DHCP required state can cause traffic to not be forwarded properly if a client is deauthenticated or removed. To overcome this, ensure that DHCP required state is always in disabled state.

Note

Starting in release 7.0.116.0 release, when the DHCP lease on the controller for internal DHCP server is cleared, the associated access points reboots.

External DHCP Servers

The operating system is designed to appear as a DHCP Relay to the network and as a DHCP server to clients with industry-standard external DHCP servers that support DHCP Relay, which means that each controller appears as a DHCP Relay agent to the DHCP server and as a DHCP server at the virtual IP address to wireless clients.

Because the controller captures the client IP address obtained from a DHCP server, it maintains the same IP address for that client during intra-controller, inter-controller, and inter-subnet client roaming.
DHCP Assignment

You can configure DHCP on a per-interface or per-WLAN basis. The preferred method is to use the primary DHCP server address assigned to a particular interface.

Per-Interface Assignment

You can assign DHCP servers for individual interfaces. The management interface, AP-manager interface, and dynamic interfaces can be configured for a primary and secondary DHCP server, and the service-port interface can be configured to enable or disable DHCP servers.

Note

See Chapter 10, “Managing Controller Software and Configurations,” for information on configuring the controller’s interfaces.

Per-WLAN Assignment

You can also define a DHCP server on a WLAN. This server will override the DHCP server address on the interface assigned to the WLAN.

Security Considerations

For enhanced security, we recommend that you require all clients to obtain their IP addresses from a DHCP server. To enforce this requirement, all WLANs can be configured with a DHCP Addr. Assignment Required setting, which disallows client static IP addresses. If DHCP Addr. Assignment Required is selected, clients must obtain an IP address via DHCP. Any client with a static IP address is not be allowed on the network. The controller monitors DHCP traffic because it acts as a DHCP proxy for the clients.

Note

WLANs that support management over wireless must allow management (device-servicing) clients to obtain an IP address from a DHCP server. See the “Using Management over Wireless” section on page 6-58 for instructions on configuring management over wireless.

If slightly less security is tolerable, you can create WLANs with DHCP Addr. Assignment Required disabled. Clients then have the option of using a static IP address or obtaining an IP address from a designated DHCP server.

Note

DHCP Addr. Assignment Required is not supported for wired guest LANs.

You are also allowed to create separate WLANs with DHCP Addr. Assignment Required being disabled. This is applicable only if DHCP proxy is enabled for the controller. It is not necessary to define the primary/secondary DHCP server. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

Note

See Chapter 4, “Configuring Controller Settings,” for instructions on globally configuring DHCP proxy.
This section provides both GUI and CLI instructions for configuring DHCP.

**Using the GUI to Configure DHCP**

To configure DHCP using the controller GUI, follow these steps:

**Step 1**
Follow the instructions in the “Configuring the Management, AP-Manager, Virtual, and Service-Port Interfaces” section on page 3-11 or “Using the GUI to Configure Dynamic Interfaces” section on page 3-18 to configure a primary DHCP server for a management, AP-manager, or dynamic interface that will be assigned to the WLAN.

**Note**
When you want to use the internal DHCP server, you must set the management interface IP address of the controller as the DHCP server IP address.

**Step 2**
Choose WLANs to open the WLANs page.

**Step 3**
Click the ID number of the WLAN for which you want to assign an interface. The WLANs > Edit (General) page appears.

**Step 4**
On the General tab, unselect the **Status** check box and click **Apply** to disable the WLAN.

**Step 5**
Reclick the ID number of the WLAN.

**Step 6**
On the General tab, choose the interface for which you configured a primary DHCP server to be used with this WLAN from the Interface drop-down list.

**Step 7**
Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page.

**Step 8**
If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, select the **DHCP Server Override** check box and enter the IP address of the desired DHCP server in the **DHCP Server IP Addr** text box. The default value for the check box is disabled.

**Note**
The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override.

**Note**
DHCP Server override is applicable only for the default group.

**Note**
If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.
The diagnostic channel enables you to troubleshoot problems regarding client communication with a WLAN. You can use the controller GUI or CLI to enable the diagnostic channel. When the diagnostic channel is “enabled” for a WLAN, the other two fields “DHCP Address Assignment Required” and “DHCP override” fields are also enabled automatically. You can use the controller GUI or CLI to disable the diagnostic channel, the two DHCP fields need to be disabled manually if you are using the GUI and if you are disabling using the CLI, the two DHCP fields gets automatically disabled.

Step 9 If you want to require all clients to obtain their IP addresses from a DHCP server, select the DHCP Addr. Assignment Required check box. When this feature is enabled, any client with a static IP address is not allowed on the network. The default value is disabled.

Note DHCP Addr. Assignment Required is not supported for wired guest LANs.

Step 10 Click Apply to commit your changes.
Step 11 On the General tab, select the Status check box and click Apply to reenable the WLAN.
Step 12 Click Save Configuration to save your changes.

Using the CLI to Configure DHCP

To configure DHCP using the controller CLI, follow these steps:

Step 1 Follow the instructions in the “Configuring the Management, AP-Manager, Virtual, and Service-Port Interfaces” section on page 3-11 or “Using the GUI to Configure Dynamic Interfaces” section on page 3-18 to configure a primary DHCP server for a management, AP-manager, or dynamic interface that will be assigned to the WLAN.

Step 2 Disable the WLAN by entering this command:

```
config wlan disable wlan_id
```

Step 3 Specify the interface for which you configured a primary DHCP server to be used with this WLAN by entering this command:

```
config wlan interface wlan_id interface_name
```

Step 4 If you want to define a DHCP server on the WLAN that will override the DHCP server address on the interface assigned to the WLAN, enter this command:

```
config wlan dhcp_server wlan_id dhcp_server_ip_address
```

Note The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the show wlan command to verify that the DHCP server has been assigned to the WLAN.
Note

If a WLAN has the DHCP server override option enabled and the controller has DHCP proxy enabled, any interface mapped to the WLAN must have a DHCP server IP address or the WLAN must be configured with a DHCP server IP address.

Step 5

Reenable the WLAN by entering this command:

```
config wlan enable wlan_id
```

Using the CLI to Debug DHCP

Use these CLI commands to obtain debug information:

- `debug dhcp packet {enable | disable}` — Enables or disables debugging of DHCP packets.
- `debug dhcp message {enable | disable}` — Enables or disables debugging of DHCP error messages.
- `debug dhcp service-port {enable | disable}` — Enables or disables debugging of DHCP packets on the service port.

Configuring DHCP Scopes

Controllers have built-in DHCP relay agents. However, when you desire network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes that assign IP addresses and subnet masks to wireless clients. Typically, one controller can have one or more DHCP scopes that each provide a range of IP addresses.

DHCP scopes are needed for internal DHCP to work. Once DHCP is defined on the controller, you can then point the primary DHCP server IP address on the management, AP-manager, and dynamic interfaces to the controller’s management interface. You can configure up to 16 DHCP scopes using the controller GUI or CLI.

Using the GUI to Configure DHCP Scopes

To configure DHCP scopes using the controller GUI, follow these steps:

Step 1

Choose Controller > Internal DHCP Server > DHCP Scope to open the DHCP Scopes page (see Figure 7-5).

Figure 7-5 DHCP Scopes Page

![DHCP Scopes Page](image)

This page lists any DHCP scopes that have already been configured.
Step 2 Click **New** to add a new DHCP scope. The DHCP Scope > New page appears.

Step 3 In the Scope Name text box, enter a name for the new DHCP scope.

Step 4 Click **Apply**. When the DHCP Scopes page reappears, click the name of the new scope. The DHCP Scope > Edit page appears (see **Figure 7-6**).

**Figure 7-6  DHCP Scope > Edit Page**

<table>
<thead>
<tr>
<th>Controller</th>
<th>DHCP Scope &gt; Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Inventory</td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td></td>
</tr>
<tr>
<td>Multicast</td>
<td></td>
</tr>
<tr>
<td>Network Routes</td>
<td></td>
</tr>
<tr>
<td>Internal DHCP Server</td>
<td></td>
</tr>
<tr>
<td>DHCP Scope</td>
<td></td>
</tr>
<tr>
<td>DHCP Allocated Leases</td>
<td></td>
</tr>
<tr>
<td>Mobility Management</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td></td>
</tr>
<tr>
<td>CDP</td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
</tbody>
</table>

Note: If you ever want to delete an existing DHCP scope, hover your cursor over the blue drop-down arrow for that scope and choose **Remove**.

Step 5 In the Pool Start Address text box, enter the starting IP address in the range assigned to the clients.

Note: This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 6 In the Pool End Address text box, enter the ending IP address in the range assigned to the clients.

Note: This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 7 In the Network text box, enter the network served by this DHCP scope. This IP address is used by the management interface with Netmask applied, as configured on the Interfaces page.

Step 8 In the Netmask text box, enter the subnet mask assigned to all wireless clients.

Step 9 In the Lease Time text box, enter the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client.

Step 10 In the Default Routers text box, enter the IP address of the optional router connecting the controllers. Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 11 In the DNS Domain Name text box, enter the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers.
Step 12 In the DNS Servers text box, enter the IP address of the optional DNS server. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.

Step 13 In the Netbios Name Servers text box, enter the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server.

Step 14 From the Status drop-down list, choose Enabled to enable this DHCP scope or choose Disabled to disable it.

Step 15 Click Apply to commit your changes.

Step 16 Click Save Configuration to save your changes.

Step 17 Choose DHCP Allocated Leases to see the remaining lease time for wireless clients. The DHCP Allocated Lease page appears (see Figure 7-7), showing the MAC address, IP address, and remaining lease time for the wireless clients.

Figure 7-7 DHCP Allocated Lease Page

![DHCP Allocated Lease Page]

Using the CLI to Configure DHCP Scopes

To configure DHCP scopes using the controller CLI, follow these steps:

Step 1 Create a new DHCP scope by entering this command:

```
config dhcp create-scope scope
```

**Note** If you ever want to delete a DHCP scope, enter this command: `config dhcp delete-scope scope`.

Step 2 Specify the starting and ending IP address in the range assigned to the clients by entering this command:

```
config dhcp address-pool scope start end
```

**Note** This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.

Step 3 Specify the network served by this DHCP scope (the IP address used by the management interface with the Netmask applied) and the subnet mask assigned to all wireless clients by entering this command:

```
config dhcp network scope network netmask
```

Step 4 Specify the amount of time (from 0 to 65536 seconds) that an IP address is granted to a client by entering this command:

```
config dhcp lease scope lease_duration
```

Step 5 Specify the IP address of the optional router connecting the controllers by entering this command:
config dhcp default-router scope router_1 [router_2] [router_3]

Each router must include a DHCP forwarding agent, which allows a single controller to serve the clients of multiple controllers.

Step 6 Specify the optional domain name system (DNS) domain name of this DHCP scope for use with one or more DNS servers by entering this command:

config dhcp domain scope domain

Step 7 Specify the IP address of the optional DNS server(s) by entering this command:

config dhcp dns-servers scope dns1 [dns2] [dns3]

Each DNS server must be able to update a client’s DNS entry to match the IP address assigned by this DHCP scope

Step 8 Specify the IP address of the optional Microsoft Network Basic Input Output System (NetBIOS) name server, such as the Internet Naming Service (WINS) server by entering this command:

config dhcp netbios-name-server scope wins1 [wins2] [wins3]

Step 9 Enable or disable this DHCP scope by entering this command:

config dhcp {enable | disable} scope

Step 10 Save your changes by entering this command:

save config

Step 11 See the list of configured DHCP scopes by entering this command:

show dhcp summary

Information similar to the following appears:

<table>
<thead>
<tr>
<th>Scope Name</th>
<th>Enabled</th>
<th>Address Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope 1</td>
<td>No</td>
<td>0.0.0.0 -&gt; 0.0.0.0</td>
</tr>
<tr>
<td>Scope 2</td>
<td>No</td>
<td>0.0.0.0 -&gt; 0.0.0.0</td>
</tr>
</tbody>
</table>

Step 12 Display the DHCP information for a particular scope by entering this command:

show dhcp scope

Information similar to the following appears:

Enabled....................................... No
Lease Time..................................... 0
Pool Start.................................... 0.0.0.0
Pool End...................................... 0.0.0.0
Network....................................... 0.0.0.0
Netmask....................................... 0.0.0.0
Default Routers............................... 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain....................................
DNS........................................... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers.......................... 0.0.0.0 0.0.0.0 0.0.0.0

---

**Configuring MAC Filtering for WLANs**

When you use MAC filtering for client or administrator authorization, you need to enable it at the WLAN level first. If you plan to use local MAC address filtering for any WLAN, use the commands in this section to configure MAC filtering for a WLAN.
Enabling MAC Filtering

Use these commands to enable MAC filtering on a WLAN:

- Enable MAC filtering by entering the `config wlan mac-filtering enable wlan_id` command.
- Verify that you have MAC filtering enabled for the WLAN by entering the `show wlan` command.

When you enable MAC filtering, only the MAC addresses that you add to the WLAN are allowed to join the WLAN. MAC addresses that have not been added are not allowed to join the WLAN.

Creating a Local MAC Filter

Controllers have built-in MAC filtering capability, similar to that provided by a RADIUS authorization server.

Use these commands to add MAC addresses to a WLAN MAC filter:

- Create a MAC filter entry on the controller by entering the `config macfilter add mac_addr wlan_id [interface_name] [description] [IP_addr]` command.
  
  The following parameters are optional:
  - `mac_addr`—MAC address of the client.
  - `wlan_id`—WLAN id on which the client is associating.
  - `interface_name`—The name of the interface. This interface name is used to override the interface configured to the WLAN.
  
  **Note** You must have AAA enabled on the WLAN to override the interface name.
  
  - `description`—A brief description of the interface in double quotes (for example, “Interface1”).
  - `IP_addr`—The IP address which is used for a passive client with the MAC address specified by the `mac_addr` value above.

- Assign an IP address to an existing MAC filter entry, if one was not assigned in the `config macfilter add` command by entering the `config macfilter ip-address mac_addr IP_addr` command.
- Verify that MAC addresses are assigned to the WLAN by entering the `show macfilter` command.

Configuring a Timeout for Disabled Clients

You can configure a timeout for disabled clients. Clients who fail to authenticate three times when attempting to associate are automatically disabled from further association attempts. After the timeout period expires, the client is allowed to retry authentication until it associates or fails authentication and is excluded again. Use these commands to configure a timeout for disabled clients:

- Configure the timeout for disabled clients by entering the `config wlan exclusionlist wlan_id timeout` command. Enter a timeout from 1 to 65535 seconds, or enter 0 to permanently disable the client.
- Verify the current timeout by entering the `show wlan` command.

Assigning WLANs to Interfaces

Use these commands to assign a WLAN to an interface:
Chapter 7      Configuring WLANs

Configuring DHCP

Assign a WLAN to an interface by entering this command:

```
config wlan interface {wlan_id | foreignAp} interface_id
```

- Use the `interface_id` option to assign the WLAN to a specific interface.
- Use the `foreignAp` option to use a third-party access point.
- Verify the interface assignment status by entering the `show wlan summary` command.

Configuring the DTIM Period

In 802.11a/n and 802.11b/g/n networks, lightweight access points broadcast a beacon at regular intervals, which coincides with the Delivery Traffic Indication Map (DTIM). After the access point broadcasts the beacon, it transmits any buffered broadcast and multicast frames based on the value set for the DTIM period. This feature allows power-saving clients to wake up at the appropriate time if they are expecting broadcast or multicast data.

Typically, the DTIM value is set to 1 (transmit broadcast and multicast frames after every beacon) or 2 (transmit after every other beacon). For instance, if the beacon period of the 802.11a/n or 802.11b/g/n network is 100 ms and the DTIM value is set to 1, the access point transmits buffered broadcast and multicast frames 10 times per second. If the beacon period is 100 ms and the DTIM value is set to 2, the access point transmits buffered broadcast and multicast frames 5 times per second. Either of these settings may be suitable for applications, including VoIP, that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (transmit broadcast and multicast frames after every 255th beacon) if all 802.11a/n or 802.11b/g/n clients have power save enabled. Because the clients have to listen only when the DTIM period is reached, they can be set to listen for broadcasts and multicasts less frequently, resulting in a longer battery life. For instance, if the beacon period is 100 ms and the DTIM value is set to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds, allowing the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, resulting in a longer battery life.

**Note**

A beacon period, which is specified in milliseconds on the controller, is converted internally by the software to 802.11 Time Units (TUs), where 1 TU = 1.024 milliseconds. On Cisco’s 802.11n access points, this value is rounded to the nearest multiple of 17 TUs. Because of this, a configured beacon period of 100 ms, for example, will result in an actual beacon period of 104 ms.

Many applications cannot tolerate a long time between broadcast and multicast messages, which results in poor protocol and application performance. We recommend a low DTIM value for 802.11a/n and 802.11b/g/n networks that support such clients.

In controller software release 5.0 or later releases, you can configure the DTIM period for the 802.11a/n and 802.11b/g/n radio networks on specific WLANs. In previous software releases, the DTIM period was configured per radio network only, not per WLAN. The benefit of this change is that now you can configure a different DTIM period for each WLAN. For example, you might want to set different DTIM values for voice and data WLANs.

**Note**

When you upgrade the controller software to release 5.0 or later releases, the DTIM period that was configured for a radio network is copied to all of the existing WLANs on the controller.
Using the GUI to Configure the DTIM Period

To configure the DTIM period for a WLAN using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure the DTIM period.

**Step 3** Unselect the Status check box to disable the WLAN.

**Step 4** Click Apply to commit your changes.

**Step 5** Choose the Advanced tab to open the WLANs > Edit (Advanced) page (see Figure 7-8).

**Figure 7-8 WLANs > Edit (Advanced) Page**

**Step 6** Under DTIM Period, enter a value between 1 and 255 (inclusive) in the 802.11a/n and 802.11b/g/n text boxes. The default value is 1 (transmit broadcast and multicast frames after every beacon).

**Step 7** Click Apply to commit your changes.

**Step 8** Choose the General tab to open the WLANs > Edit (General) page.

**Step 9** Select the Status check box to reenable the WLAN.

**Step 10** Click Save Configuration to save your changes.

Using the CLI to Configure the DTIM Period

To configure the DTIM period for a WLAN using the controller CLI, follow these steps:

**Step 1** Disable the WLAN by entering this command:
```
config wlan disable wlan_id
```

**Step 2** Configure the DTIM period for either the 802.11a/n or 802.11b/g/n radio network on a specific WLAN by entering this command:
```
config wlan dtim (802.11a | 802.11b) dtim wlan_id
```

where dtim is a value between 1 and 255 (inclusive). The default value is 1 (transmit broadcast and multicast frames after every beacon).
Step 3  Reenable the WLAN by entering this command:

```
config wlan enable wlan_id
```

Step 4  Save your changes by entering this command:

```
save config
```

Step 5  Verify the DTIM period by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier........................... 1
Profile Name................................. employee
Network Name (SSID)......................... employee
Status........................................ Enabled
...
DTIM period for 802.11a radio............... 1
DTIM period for 802.11b radio.............. 1
Local EAP Authentication.................... Disabled
...
```

### Configuring Peer-to-Peer Blocking

In controller software releases prior to 4.2, peer-to-peer blocking is applied globally to all clients on all WLANs and causes traffic between two clients on the same VLAN to be transferred to the upstream VLAN rather than being bridged by the controller. This behavior usually results in traffic being dropped at the upstream switch because switches do not forward packets out the same port on which they are received.

In controller software release 4.2 or later releases, peer-to-peer blocking is applied to individual WLANs, and each client inherits the peer-to-peer blocking setting of the WLAN to which it is associated. In software release 4.2 or later releases, you also have more control over how traffic is directed. For example, you can choose to have traffic bridged locally within the controller, dropped by the controller, or forwarded to the upstream VLAN. Figure 7-9 shows each option.

**Note**

Peer-to-peer blocking will not work across the clients in different WLANs which are mapped to the same VLAN. For example, if WLAN-1 and WLAN-2 are mapped to the same interface say VLAN-1, then peer-to-peer blocking will not work. The WLAN-1 + WLAN-2 are configured with peer-to-peer blocking action in the WLAN as DROP. Clients in WLAN-1 will not be able to pass the traffic to clients in WLAN-2.
Figure 7-9  Peer-to-Peer Blocking Examples

Guidelines for Using Peer-to-Peer Blocking

Follow these guidelines when using peer-to-peer blocking:

- In controller software releases prior to 4.2, the controller forwards Address Resolution Protocol (ARP) requests upstream (just like all other traffic). In controller software release 4.2 or later releases, ARP requests are directed according to the behavior set for peer-to-peer blocking.
- Peer-to-peer blocking does not apply to multicast traffic.
- Locally switched hybrid-REAP WLANs and hybrid-REAP access points in standalone mode do not support peer-to-peer blocking.
- If you upgrade to controller software release 4.2 or later releases from a previous release that supports global peer-to-peer blocking, each WLAN is configured with the peer-to-peer blocking action of forwarding traffic to the upstream VLAN.

Using the GUI to Configure Peer-to-Peer Blocking

To configure a WLAN for peer-to-peer blocking using the controller GUI, follow these steps:

**Step 1**  Choose WLANs to open the WLANs page.

**Step 2**  Click the ID number of the WLAN for which you want to configure peer-to-peer blocking.

**Step 3**  Choose the Advanced tab to open the WLANs > Edit (Advanced) page (see Figure 7-10).
Configuring DHCP

Chapter 7      Configuring WLANs

Step 4  Choose one of the following options from the P2P Blocking drop-down list:

- **Disabled**—Disables peer-to-peer blocking and bridges traffic locally within the controller whenever possible. This is the default value.

  **Note** Traffic is never bridged across VLANs in the controller.

- **Drop**—Causes the controller to discard the packets.

- **Forward-UpStream**—Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.

Step 5  Click **Apply** to commit your changes.

Step 6  Click **Save Configuration** to save your changes.

Using the CLI to Configure Peer-to-Peer Blocking

To configure a WLAN for peer-to-peer blocking using the controller CLI, follow these steps:

Step 1  Configure a WLAN for peer-to-peer blocking by entering this command:

```bash
config wlan peer-blocking {disable | drop | forward-upstream} wlan_id
```

  **Note** See the description of each parameter in the “Using the GUI to Configure Peer-to-Peer Blocking” section above.

Step 2  Save your changes by entering this command:

```bash
save config
```

Step 3  See the status of peer-to-peer blocking for a WLAN by entering this command:

```bash
show wlan wlan_id
```

Information similar to the following appears:
Chapter 7  Configuring WLANs

Configuring Layer 2 Security

This section describes how to assign Layer 2 security settings to WLANs.

Static WEP Keys

Controllers can control static WEP keys across access points. Use these commands to configure static WEP for WLANs:

- Disable the 802.1X encryption by entering this command:

  `config wlan security 802.1X disable wlan_id`

- Configure 40/64-bit or 104/128-bit WEP keys by entering this command:

  `config wlan security static-wep-key encryption wlan_id { 40 | 104 } { hex | ascii } key key_index`

  - Use the `40` or `104` option to specify 40/64-bit or 104/128-bit encryption. The default setting is 104/128.
  - Use the `hex` or `ascii` option to specify the character format for the WEP key.
  - Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F) or five printable ASCII characters for 40-bit/64-bit WEP keys or enter 26 hexadecimal or 13 ASCII characters for 104-bit/128-bit keys.
  - Enter a key index (sometimes called a key slot). The default value is 0, which corresponds to a key index of 1; the valid values are 0 to 3 (key index of 1 to 4).

Dynamic 802.1X Keys and Authorization

Controllers can control 802.1X dynamic WEP keys using Extensible Authentication Protocol (EAP) across access points and support 802.1X dynamic key settings for WLANs.

\[\text{Note}\]

To use LEAP with lightweight access points and wireless clients, make sure to choose Cisco-Aironet as the RADIUS server type when configuring the CiscoSecure Access Control Server (ACS).

- Check the security settings of each WLAN by entering this command:

  `show wlan wlan_id`

  The default security setting for new WLANs is 802.1X with dynamic keys enabled. To maintain robust Layer 2 security, leave 802.1X configured on your WLANs.

- Disable or enable the 802.1X authentication by entering this command:
config wlan security 802.1X {enable | disable} wlan_id

After you enable 802.1X authentication, the controller sends EAP authentication packets between the wireless client and the authentication server. This command allows all EAP-type packets to be sent to and from the controller.

- Change the 802.1X encryption level for a WLAN by entering this command:

  config wlan security 802.1X encryption wlan_id [0 | 40 | 104]
  - Use the 0 option to specify no 802.1X encryption.
  - Use the 40 option to specify 40/64-bit encryption.
  - Use the 104 option to specify 104/128-bit encryption. (This is the default encryption setting.)

Configuring a WLAN for Both Static and Dynamic WEP

You can configure up to four WLANs to support static WEP keys, and you can also configure dynamic WEP on any of these static-WEP WLANs. Follow these guidelines when configuring a WLAN for both static and dynamic WEP:

- The static WEP key and the dynamic WEP key must be the same length.
- When you configure both static and dynamic WEP as the Layer 2 security policy, no other security policies can be specified. That is, you cannot configure web authentication. However, when you configure either static or dynamic WEP as the Layer 2 security policy, you can configure web authentication.

WPA1 and WPA2

Wi-Fi Protected Access (WPA or WPA1) and WPA2 are standards-based security solutions from the Wi-Fi Alliance that provide data protection and access control for wireless LAN systems. WPA1 is compatible with the IEEE 802.11i standard but was implemented prior to the standard’s ratification; WPA2 is the Wi-Fi Alliance’s implementation of the ratified IEEE 802.11i standard.

The following are some of the Layer 2 Security methods that a client can use to log on to a wireless system:

- 801X—This includes:
  - Original 802.1x authentication method
  - No rekeying method; wireless clients must authenticate to the RADIUS server every time they associate to a new AP
  - Dynamic WEP (can be configured with static WEP) for data protection

- WPA1—This includes:
  - 802.1x EAP based authentication method: LEAP, EAP-FAST, PEAP, EAP-TLS
  - PSK, 802.1x, and CCKM rekeying mechanisms
  - Temporal Key Integrity Protocol (TKIP) (dynamic WEP encryption) with message integrity check (MIC) for data protection

- WPA2—This includes:
  - 802.1x EAP based authentication method: LEAP, EAP-FAST, PEAP, EAP-TLS
  - PSK, 802.1x, and CCKM rekeying mechanisms
The following are the rekeying mechanisms used by both WPA1 and WPA2, with the default being 802.1X:

- **802.1X**—802.11i International Engineering Task Force (IETF) standard rekeying mechanism. We recommend this mechanism for non-Cisco hardware clients.
- **PSK**—When you choose PSK (also known as WPA preshared key or WPA passphrase), you need to configure a preshared key (or a passphrase). This key is used as the pairwise master key (PMK) between the clients and the authentication server.
- **CCKM**—Cisco Centralized Key Management (CCKM) uses a fast rekeying technique that enables clients to roam from one access point to another without going through the controller, typically in under 150 milliseconds (ms). CCKM reduces the time required by the client to mutually authenticate with the new access point and derive a new session key during reassociation. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications such as wireless Voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions. CCKM is a CCXv4-compliant feature. If CCKM is selected, only CCKM clients are supported.

When CCKM is enabled, the behavior of access points differs from the controller's for fast roaming in the following ways:

- If an association request sent by a client has CCKM enabled in a Robust Secure Network Information Element (RSN IE) but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then the controller does not do a full authentication. Instead, the controller validates the PMKID and does a four-way handshake.
- If an association request sent by a client has CCKM enabled in RSN IE but CCKM IE is not encoded and only PMKID is encoded in RSN IE, then AP does a full authentication. The access point does not use PMKID sent with the association request when CCKM is enabled in RSN IE.

**Note**
The OEAP 600 series does not support fast roaming for clients. Dual mode voice clients will experience reduced call quality when they roam between the two spectrums on OEAP602 access point. We recommend that you configure voice devices to only connect on one band, either 2.4 GHz or 5.0 GHz.

**Note**
The 4.2 or later release of controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit client functionality. Clients must support CCXv4 or v5 in order to use CCKM. See the “Configuring Cisco Client Extensions” section on page 7-53 for more information on CCX.

- **802.1X+CCKM**—During normal operation, 802.1X-enabled clients mutually authenticate with a new access point by performing a complete 802.1X authentication, including communication with the main RADIUS server. However, when you configure your WLAN for 802.1X and CCKM fast secure roaming, CCKM-enabled clients securely roam from one access point to another without the need to reauthenticate to the RADIUS server. 802.1X+CCKM is considered optional CCKM because both CCKM and non-CCKM clients are supported when this option is selected.
When the AP advertises its security capabilities via the Robust Security Network Information Element (RSNIE) in the beacons and probe responses of the access point, CCKM rekeying capability is communicated by a MAC organizationally unique identifier (OUI) value of 00:40:96 and a type value of 0 in the Authenticated Key Management (AKM) suite selector of the RSNIE. 802.1x rekeying mechanism uses the MAC OUI of 00:0f:ac and a type value of 1 in the AKM suite selector of the RSNIE. The PSK uses a MAC OUI of 00:0f:ac with a type value of 6 in the AKM suite selector of the RSNIE.

On a single WLAN, you can allow WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM clients to join. All of the access points on such a WLAN advertise WPA1, WPA2, and 802.1X/PSK/CCKM/802.1X+CCKM information elements in their beacons and probe responses. When you enable WPA1 and/or WPA2, you can also enable one or two ciphers, or cryptographic algorithms, designed to protect data traffic. Specifically, you can enable AES and/or TKIP data encryption for WPA1 and/or WPA2. TKIP is the default value for WPA1, and AES is the default value for WPA2.

Note

WLAN should be enabled only after WPA1 and WPA2 ciphers are enabled. You can enable WPA1 and WPA2 using the `config wlan security wpa {wpa1/wpa2} enable` command. You cannot enable ciphers from the GUI unless WPA1 and WPA2 are enabled.

Using the GUI to Configure WPA1+WPA2

To configure a WLAN for WPA1+WPA2 using the controller GUI, follow these steps:

Step 1 Choose WLANs to open the WLANs page.
Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.
Step 3 Choose the Security and Layer 2 tabs to open the WLANs > Edit (Security > Layer 2) page (see Figure 7-11).

Figure 7-11 WLANs > Edit (Security > Layer 2) Page

Step 4 Choose WPA+WPA2 from the Layer 2 Security drop-down list.
Step 5 Under WPA+WPA2 Parameters, select the WPA Policy check box to enable WPA1, select the WPA2 Policy check box to enable WPA2, or select both check boxes to enable both WPA1 and WPA2.
Configuring DHCP

Note The default value is disabled for both WPA1 and WPA2. If you leave both WPA1 and WPA2 disabled, the access points advertise in their beacons and probe responses information elements only for the authentication key management method that you choose in Step 7.

Step 6 Select the AES check box to enable AES data encryption or the TKIP check box to enable TKIP data encryption for WPA1, WPA2, or both. The default values are TKIP for WPA1 and AES for WPA2.

Step 7 Choose one of the following key management methods from the Auth Key Mgmt drop-down list: 802.1X, CCKM, PSK, or 802.1X+CCKM.

Note Cisco OEAP 600 does not support CCKM. You must choose either 802.1X or PSK.

Note For Cisco OEAP 600, the TKIP and AES security encryption settings must be identical for WPA and WPA2.

Step 8 If you chose PSK in Step 7, choose ASCII or HEX from the PSK Format drop-down list and then enter a preshared key in the blank text box. WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

Note The PSK parameter is a set-only parameter. The value set for the PSK key is not visible to the user for security reasons. For example, if you selected HEX as the key format when setting the PSK key, and later when you view the parameters of this WLAN, the value shown is the default value. The default is ASCII.

Step 9 Click Apply to commit your changes.

Step 10 Click Save Configuration to save your changes.

Using the CLI to Configure WPA1+WPA2

To configure a WLAN for WPA1+WPA2 using the controller CLI, follow these steps:

Step 1 Disable the WLAN by entering this command:

```
config wlan disable wlan_id
```

Step 2 Enable or disable WPA for the WLAN by entering this command:

```
config wlan security wpa {enable | disable} wlan_id
```

Step 3 Enable or disable WPA1 for the WLAN by entering this command:

```
config wlan security wpa wpa1 {enable | disable} wlan_id
```

Step 4 Enable or disable WPA2 for the WLAN by entering this command:

```
config wlan security wpa wpa2 {enable | disable} wlan_id
```

Step 5 Enable or disable AES or TKIP data encryption for WPA1 or WPA2 by entering one of these commands:

- config wlan security wpa wpa1 ciphers {aes | tkip} {enable | disable} wlan_id
Chapter 7 Configuring WLANs

Configuring DHCP

- `config wlan security wpa wpa2 ciphers {aes | tkip} {enable | disable} wlan_id`

  The default values are TKIP for WPA1 and AES for WPA2.

**Step 6**

Enable or disable 802.1X, PSK, or CCKM authenticated key management by entering this command:

`config wlan security wpa akm {802.1X | psk | cckm} {enable | disable} wlan_id`

The default value is 802.1X.

**Step 7**

If you enabled PSK in Step 6, enter this command to specify a preshared key:

`config wlan security wpa akm psk set-key {ascii | hex} psk-key wlan_id`

WPA preshared keys must contain 8 to 63 ASCII text characters or 64 hexadecimal characters.

**Step 8**

If you enabled WPA2 with 802.1X authenticated key management or WPA1 or WPA2 with CCKM authenticated key management, the PMK cache lifetime timer is used to trigger reauthentication with the client when necessary. The timer is based on the timeout value received from the AAA server or the WLAN session timeout setting. To see the amount of time remaining before the timer expires, enter this command:

`show pmk-cache all`

Information similar to the following appears:

```
PMK-CCKM Cache

<table>
<thead>
<tr>
<th>Type</th>
<th>Station</th>
<th>Lifetime</th>
<th>VLAN Override</th>
<th>IP Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCKM</td>
<td>00:07:0e:b9:3a:1b</td>
<td>150</td>
<td></td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
```

If you enabled WPA2 with 802.1X authenticated key management, the controller supports opportunistic PMKID caching but not sticky (or non-opportunistic) PMKID caching. In sticky PMKID caching, the client stores multiple PMKIDs. This approach is not practical because it requires full authentication for each new access point and is not guaranteed to work in all conditions. In contrast, opportunistic PMKID caching stores only one PMKID per client and is not subject to the limitations of sticky PMK caching.

**Step 9**

Enable the WLAN by entering this command:

`config wlan enable wlan_id`

**Step 10**

Save your settings by entering this command:

`save config`

---

**CKIP**

Cisco Key Integrity Protocol (CKIP) is a Cisco-proprietary security protocol for encrypting 802.11 media. CKIP improves 802.11 security in infrastructure mode using key permutation, a message integrity check (MIC), and a message sequence number. Software release 4.0 or later releases support CKIP with a static key. For this feature to operate correctly, you must enable Aironet information elements (IEs) for the WLAN.

A lightweight access point advertises support for CKIP in beacon and probe response packets by adding an Aironet IE and setting one or both of the CKIP negotiation bits (key permutation and multi-modular hash message integrity check [MMH MIC]). Key permutation is a data encryption technique that uses the basic encryption key and the current initialization vector (IV) to create a new key. MMH MIC prevents bit-flip attacks on encrypted packets by using a hash function to compute message integrity code.
The CKIP settings specified in a WLAN are mandatory for any client attempting to associate. If the WLAN is configured for both CKIP key permutation and MMH MIC, the client must support both. If the WLAN is configured for only one of these features, the client must support only the CKIP feature.

CKIP requires that 5-byte and 13-byte encryption keys be expanded to 16-byte keys. The algorithm to perform key expansion occurs at the access point. The key is appended to itself repeatedly until the length reaches 16 bytes. All lightweight access points support CKIP.

You can configure CKIP through either the GUI or the CLI.

### Using the GUI to Configure CKIP

To configure a WLAN for CKIP using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the desired WLAN to open the WLANs > Edit page.

**Step 3** Choose the Advanced tab.

**Step 4** Select the Aironet IE check box to enable Aironet IEs for this WLAN and click Apply.

**Step 5** Choose the General tab.

**Step 6** Unselect the Status check box, if selected, to disable this WLAN and click Apply.

**Step 7** Choose the Security and Layer 2 tabs to open the WLANs > Edit (Security > Layer 2) page (see Figure 7-12).

**Step 8** Choose CKIP from the Layer 2 Security drop-down list.

**Step 9** Under CKIP Parameters, choose the length of the CKIP encryption key from the Key Size drop-down list. The range is Not Set, 40 bits, or 104 bits and the default is Not Set.

**Step 10** Choose the number to be assigned to this key from the Key Index drop-down list. You can configure up to four keys.

**Step 11** From the Key Format drop-down list, choose ASCII or HEX and then enter an encryption key in the Encryption Key text box. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
Step 12 Select the **MMH Mode** check box to enable MMH MIC data protection for this WLAN. The default value is disabled (or unselected).

Step 13 Select the **Key Permutation** check box to enable this form of CKIP data protection. The default value is disabled (or unselected).

Step 14 Click **Apply** to commit your changes.

Step 15 Choose the **General** tab.

Step 16 Select the **Status** check box to enable this WLAN.

Step 17 Click **Apply** to commit your changes.

Step 18 Click **Save Configuration** to save your changes.

**Using the CLI to Configure CKIP**

To configure a WLAN for CKIP using the controller CLI, follow these steps:

**Step 1** Disable the WLAN by entering this command:
```
config wlan disable wlan_id
```

**Step 2** Enable Aironet IEs for this WLAN by entering this command:
```
config wlan ccx aironet-ie enable wlan_id
```

**Step 3** Enable or disable CKIP for the WLAN by entering this command:
```
config wlan security ckip {enable | disable} wlan_id
```

**Step 4** Specify a CKIP encryption key for the WLAN by entering this command:
```
config wlan security ckip akm psk set-key wlan_id {40 | 104} {hex | ascii} key key_index
```

**Step 5** Enable or disable CKIP MMH MIC for the WLAN by entering this command:
```
config wlan security ckip mmh-mic {enable | disable} wlan_id
```

**Step 6** Enable or disable CKIP key permutation for the WLAN by entering this command:
```
config wlan security ckip kp {enable | disable} wlan_id
```

**Step 7** Enable the WLAN by entering this command:
```
config wlan enable wlan_id
```

**Step 8** Save your settings by entering this command:
```
save config
```

**Configuring a Session Timeout**

Using the controller GUI or CLI, you can configure a session timeout for wireless clients on a WLAN. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.
Using the GUI to Configure a Session Timeout

To configure a session timeout for wireless clients on a WLAN using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to assign a session timeout.

**Step 3** When the WLANs > Edit page appears, choose the Advanced tab. The WLANs > Edit (Advanced) page appears.

**Step 4** Select the **Enable Session Timeout** check box to configure a session timeout for this WLAN. Otherwise, unselect the check box. The default value is selected.

In the Session Timeout text box, enter a value between 300 and 86400 seconds to specify the duration of the client session. The default value is 1800 seconds for the following Layer 2 security types: 802.1X, Static WEP+802.1X, WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types (Open WLAN/CKIP/Static WEP). A value of 0 is equivalent to no timeout.

**Step 5** Click **Apply** to commit your changes.

**Step 6** Click **Save Configuration** to save your changes.

Using the CLI to Configure a Session Timeout

To configure a session timeout for wireless clients on a WLAN using the controller CLI, follow these steps:

**Step 1** Configure a session timeout for wireless clients on a WLAN by entering this command:

```
config wlan session-timeout wlan_id timeout
```

The default value is 1800 seconds for the following Layer 2 security types: 802.1X, Static WEP+802.1X, WPA+WPA2 with 802.1X, CCKM, or 802.1X+CCKM authentication key management and 0 seconds for all other Layer 2 security types (Open WLAN/CKIP/Static WEP). A value of 0 is equivalent to no timeout.

**Step 2** Save your changes by entering this command:

```
save config
```

**Step 3** See the current session timeout value for a WLAN by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier.......................... 9
Profile Name.............................. test12
Network Name (SSID)..................... test12
... Number of Active Clients........... 0
Exclusionlist Timeout.................. 60 seconds
Session Timeout......................... 1800 seconds
...
Configuring Layer 3 Security

This section describes how to configure Layer 3 security settings for a WLAN on the controller.

**Note**
- Layer 2 Tunnel Protocol (L2TP) and IPsec are not supported on controllers that run software release 4.0 or later releases.
- Layer 3 security settings are not supported when you disable the client IP address on a WLAN.

**VPN Passthrough**

The controller supports VPN passthrough or the “passing through” of packets that originate from VPN clients. An example of VPN passthrough is your laptop trying to connect to the VPN server at your corporate office.

**Note**
The VPN Passthrough option is not available on Cisco 5500 Series and Cisco 2100 Series Controllers. However, you can replicate this functionality on a Cisco 5500 or 2100 Series Controller by creating an open WLAN using an ACL.

**Using the GUI to Configure VPN Passthrough**

To configure a WLAN for VPN passthrough using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure VPN passthrough. The WLANs > Edit page appears.

**Step 3** Choose the Security and Layer 3 tabs to open the WLANs > Edit (Security > Layer 3) page.

**Step 4** From the Layer 3 Security drop-down list, choose VPN Pass-Through.

**Step 5** In the VPN Gateway Address text box, enter the IP address of the router that is terminating the VPN tunnels initiated by the client and passed through the controller.

**Step 6** Click Apply to commit your changes.

**Step 7** Click Save Configuration to save your settings.

**Using the CLI to Configure VPN Passthrough**

Configure a WLAN for VPN passthrough using the controller CLI by entering this command:

```
config wlan security passthru {enable | disable} wlan_id gateway
```

For `gateway`, enter the IP address of the router that is terminating the VPN tunnel.

Verify that the passthrough is enabled by entering this command:

```
show wlan
```
Web Authentication

WLANs can use web authentication only if VPN passthrough is not enabled on the controller. Web authentication is simple to set up and use and can be used with SSL to improve the overall security of the WLAN.

**Note**
Web authentication is supported only with these Layer 2 security policies: open authentication, open authentication+WEP, and WPA-PSK. It is not supported for use with 802.1X.

**Note**
The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

**Note**
If the CPU ACL’s are configured to block HTTP / HTTPS traffic, after the successful web login authentication, there could be a failure in the redirection page.

**Note**
Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.

**Note**
When you enable web authentication for a WLAN, a message appears indicating that the controller forwards DNS traffic to and from wireless clients prior to authentication. We recommend that you have a firewall or intrusion detection system (IDS) behind your guest VLAN to regulate DNS traffic and to prevent and detect any DNS tunneling attacks.

**Note**
When HTTP and HTTPS for management access for the controller is enabled, the webauth redirection occurs only on HTTPS. To get HTTP webauth redirection, ensure that you enable only HTTP for management access and disable HTTPS for management access.

If the web authentication is enabled on the WLAN and you also have the CPU ACL rules, the client-based web authentication rules take higher precedence as long as the client is unauthenticated (in the webAuth_Reqd state). Once the client goes to the RUN state, the CPU ACL rules get applied. Therefore, if the CPU ACL rules are enabled in the controller, an allow rule for the virtual interface IP is required (in any direction) with the following conditions:

- When the CPU ACL does not have an allow ACL rule for both directions.
- When an allow ALL rule exists, but also a DENY rule for port 443 or 80 of higher precedence.

The allow rule for the virtual IP should be for TCP protocol and port 80 (if secureweb is disabled) or port 443 (if secureweb is enabled). This process is required to allow client’s access to the virtual interface IP address, post successful authentication when the CPU ACL rules are in place.

**Note**
When clients connect to a WebAuth SSID and a preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.
Note

You can select the following identity stores to authenticate web-auth user, under WLANs > Security > AAA servers > Authentication priority order for web-auth user section:

– Local,
– RADIUS,
– LDAP

If multiple identity stores are selected, then the controller checks each identity store in the list, in the order specified, from top to bottom, until authentication for the user succeeds. The authentication fails, if the controller reaches the end of the list and user remains un-authenticated in any of the identity stores.

Using the GUI to Configure Web Authentication

To configure a WLAN for web authentication using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure web authentication. The WLANs > Edit page appears.

**Step 3** Choose the Security and Layer 3 tabs to open the WLANs > Edit (Security > Layer 3) page.

**Step 4** Select the Web Policy check box.

**Step 5** Make sure that the Authentication option is selected.

**Step 6** Click Apply to commit your changes.

**Step 7** Click Save Configuration to save your settings.

**Step 8** See Chapter 11, “Managing User Accounts,” for more information on using web authentication.

Using the CLI to Configure Web Authentication

To configure a WLAN for web authentication using the controller CLI, follow these steps:

**Step 1** Enable or disable web authentication on a particular WLAN by entering this command:

```bash
config wlan security web-auth {enable | disable} wlan_id
```

**Step 2** Release the guest user IP address when the web authentication policy timer expires and prevent the guest user from acquiring an IP address for 3 minutes by entering this command:

```bash
config wlan webauth-exclude wlan_id {enable | disable}
```

The default value is disabled. This command is applicable when you configure the internal DHCP scope on the controller. By default, when the web authentication timer expires for a guest user, the user can immediately reassociate to the same IP address before another guest user can acquire it. If there are many guest users or limited IP addresses in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user’s IP address is released when the web authentication policy timer expires and the guest user is excluded from acquiring an IP address for 3 minutes. The IP address is available for another guest user to use. After 3 minutes, the excluded guest user can reassociate and acquire an IP address, if available.

**Step 3** See the status of web authentication by entering this command:

```bash
show wlan wlan_id
```
Information similar to the following appears:

WLAN Identifier................................. 1
Profile Name...................................... cj
Network Name (SSID)............................ cj
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID.................................... Enabled
AAA Policy Override............................. Disabled
Network Admission Control

  MAC-State...................................... Disabled
  Quarantine VLAN.............................. 0
  Number of Active Clients..................... 0
  Exclusionlist Timeout........................ 60 seconds
  Session Timeout.............................. 1800 seconds
  CHD per WLAN.................................. Enabled
  Webauth DHCP exclusion....................... Disabled
  Interface...................................... management
  WLAN ACL........................................ unconfigured
  DHCP Server.................................... Default
  DHCP Address Assignment Required.......... Disabled
  ...

Web Based Authentication....................... Disabled
Web-Passthrough................................ Disabled
...

Step 4 For more information on using web authentication, see Chapter 11, “Managing User Accounts.”

Configuring a Fallback Policy with MAC Filtering and Web Authentication

You can configure a fallback policy mechanism that combines Layer 2 and Layer 3 security. In a scenario where you have both MAC filtering and web authentication implemented, when a client tries to connect to a WLAN using the MAC filter (RADIUS server), if the client fails the authentication, you can configure the authentication to fall back to web authentication. When a client passes the MAC filter authentication, the web authentication is skipped and the client is connected to the WLAN. With this feature, you can avoid disassociations based on only a MAC filter authentication failure.

Note Mac filter failure (conditional web redirect) is not defined for auto-anchor scenarios.

Using the GUI to Configure a Fallback Policy with MAC Filtering and Web Authentication

To configure a fallback policy with MAC filtering and web authentication on a WLAN using the controller GUI, follow these steps:

Note Before configuring a fallback policy, you must have MAC filtering enabled. To know more about how to enable MAC filtering, see the “Configuring MAC Filtering for WLANs” section on page 7-17.

Step 1 Choose WLANs to open the WLANs page.
Step 2 Click the ID number of the WLAN for which you want to configure the fallback policy for web authentication. The WLANs > Edit page appears.
Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page (see Figure 7-13).

### Figure 7-13 WLANs > Edit (Security > Layer 3) Page

![WLANs > Edit (Security > Layer 3) Page]

#### Step 4
- From the Layer 3 Security drop-down list, choose **None**.

#### Step 5
- Select the **Web Policy** check box.

**Note**
The controller forwards DNS traffic to and from wireless clients prior to authentication.

The following options are displayed:
- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter Failure

#### Step 6
Click **On MAC Filter Failure**.

#### Step 7
Click **Apply** to commit your changes.

#### Step 8
Click **Save Configuration** to save your settings.

---

**Using the CLI to Configure a Fallback Policy with MAC Filtering and Web Authentication**

To configure a fallback policy with MAC filtering and web authentication on a WLAN using the controller CLI, follow these steps:

**Note**
Before configuring a fallback policy, you must have MAC filtering enabled. To know more about how to enable MAC filtering, see the “Configuring MAC Filtering for WLANs” section on page 7-17.
Step 1  Enable or disable web authentication on a particular WLAN by entering this command:
config wlan security web-auth on-macfilter-failure wlan-id

Step 2  See the web authentication status by entering this command:
show wlan wlan_id

<table>
<thead>
<tr>
<th>FT Over-The-Ds mode</th>
<th>CKIP</th>
<th>IP Security</th>
<th>IP Security Passthru</th>
<th>Web Based Authentication</th>
<th>ACL</th>
<th>Web Authentication server precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Enabled-On-MACFilter-Failure</td>
<td>Unconfigured</td>
<td>local radius ldap</td>
</tr>
</tbody>
</table>

Assigning a QoS Profile to a WLAN

Cisco UWN solution WLANs support four levels of QoS: Platinum/Voice, Gold/Video, Silver/Best Effort (default), and Bronze/Background. You can configure the voice traffic WLAN to use Platinum QoS, assign the low-bandwidth WLAN to use Bronze QoS, and assign all other traffic between the remaining QoS levels.

The WLAN QoS level defines a specific 802.11e user priority (UP) for over-the-air traffic. This UP is used to derive the over-the-wire priorities for non-WMM traffic, and it also acts as the ceiling when managing WMM traffic with various levels of priorities. The access point uses this QoS-profile-specific UP in accordance with the values in Table 7-2 to derive the IP DSCP value that is visible on the wired LAN.

<table>
<thead>
<tr>
<th>AVVID Traffic Type</th>
<th>AVVID IP DSCP</th>
<th>QoS Profile</th>
<th>AVVID 802.1p</th>
<th>IEEE 802.11e UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network control</td>
<td>56 (CS7)</td>
<td>Platinum</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Inter-network control (CAPWAP control, 802.11 management)</td>
<td>48 (CS6)</td>
<td>Platinum</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Voice</td>
<td>46 (EF)</td>
<td>Platinum</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Interactive video</td>
<td>34 (AF41)</td>
<td>Gold</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Mission critical</td>
<td>26 (AF31)</td>
<td>Gold</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Transactional</td>
<td>18 (AF21)</td>
<td>Silver</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Bulk data</td>
<td>10 (AF11)</td>
<td>Bronze</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Best effort</td>
<td>0 (BE)</td>
<td>Silver</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Scavenger</td>
<td>2</td>
<td>Bronze</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

You can assign a QoS profile to a WLAN using the controller GUI or CLI.
Chapter 7      Configuring WLANs

Using the GUI to Assign a QoS Profile to a WLAN

To assign a QoS profile to a WLAN using the controller GUI, follow these steps:

Step 1 If you have not already done so, configure one or more QoS profiles using the instructions in the “Using the GUI to Configure QoS Profiles” section on page 4-65.

Step 2 Choose WLANs to open the WLANs page.

Step 3 Click the ID number of the WLAN to which you want to assign a QoS profile.

Step 4 When the WLANs > Edit page appears, choose the QoS tab.

Step 5 From the Quality of Service (QoS) drop-down list, choose one of the following:
  - Platinum (voice)
  - Gold (video)
  - Silver (best effort)
  - Bronze (background)

Note Silver (best effort) is the default value.

Step 6 Click Apply to commit your changes.

Step 7 Click Save Configuration to save your changes.

Using the CLI to Assign a QoS Profile to a WLAN

To assign a QoS profile to a WLAN using the controller CLI, follow these steps:

Step 1 If you have not already done so, configure one or more QoS profiles using the instructions in the “Using the CLI to Configure QoS Profiles” section on page 4-67.

Step 2 Assign a QoS profile to a WLAN by entering this command:

```
config wlan qos wlan_id {bronze | silver | gold | platinum}
```

Silver is the default value.

Step 3 Save your changes by entering this command:

```
save config
```

Step 4 Verify that you have properly assigned the QoS profile to the WLAN by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

---

**Note**

The IEEE 802.11e UP value for DSCP values that are not mentioned in the table is calculated by considering 3 MSB bits of DSCP. For example, the IEEE 802.11e UP value for DSCP 32 (100 000 in binary), would be the decimal converted value of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.
Configuring QoS Enhanced BSS

The QoS Enhanced Basis Service Set (QBSS) information element (IE) enables the access points to communicate their channel usage to wireless devices. Because access points with high channel usage might not be able to handle real-time traffic effectively, the 7921 or 7920 phone uses the QBSS value to determine if they should associate to another access point. You can enable QBSS in these two modes:

- Wi-Fi Multimedia (WMM) mode, which supports devices that meet the 802.11E QBSS standard (such as Cisco 7921 IP Phones)
- 7920 support mode, which supports Cisco 7920 IP Phones on your 802.11b/g network

The 7920 support mode has two options:
- Support for 7920 phones that require call admission control (CAC) to be configured on and advertised by the client device (these are typically older 7920 phones)
- Support for 7920 phones that require CAC to be configured on and advertised by the access point (these are typically newer 7920 phones)

When access point-controlled CAC is enabled, the access point sends out a Cisco proprietary CAC Information Element (IE) and does not send out the standard QBSS IE.

Note: The OEAP 600 Series access points do not support CAC.

You can use the controller GUI or CLI to configure QBSS. QBSS is disabled by default.

Guidelines for Configuring QBSS

Follow these guidelines when configuring QBSS on a WLAN:

- 7920 phones are non-WMM phones with limited CAC functionality. The phones look at the channel utilization of the access point to which they are associated and compare that to a threshold that is beaconed by the access point. If the channel utilization is less than the threshold, the 7920 places a call. In contrast, 7921 phones are full-fledged WMM phones that use traffic specifications (TSPECs)
to gain access to the voice queue before placing a phone call. The 7921 phones work well with load-based CAC, which uses the percentage of the channel set aside for voice and tries to limit the calls accordingly.

Because 7921 phones support WMM and 7920 phones do not, capacity and voice quality problems can arise if you do not properly configure both phones when they are used in a mixed environment. To enable both 7921 and 7920 phones to co-exist on the same network, make sure that load-based CAC and 7920 AP CAC are both enabled on the controller and the WMM Policy is set to Allowed. These settings become particularly important if you have many more 7920 users than 7921 users.

Note: See Chapter 4, “Configuring Controller Settings,” for more information and configuration instructions for load-based CAC.

Additional Guidelines for Using Cisco 7921 and 7920 Wireless IP Phones

Follow these guidelines to use Cisco 7921 and 7920 Wireless IP Phones with controllers:

- Aggressive load balancing must be disabled for each controller. Otherwise, the initial roam attempt by the phone may fail, causing a disruption in the audio path.

- The Dynamic Transmit Power Control (DTPC) information element (IE) must be enabled using the `config 802.11b dtpc enable` command. The DTPC IE is a beacon and probe information element that allows the access point to broadcast information on its transmit power. The 7921 or 7920 phone uses this information to automatically adjust its transmit power to the same level as the access point to which it is associated. In this manner, both devices are transmitting at the same level.

- Both the 7921 and 7920 phones and the controllers support Cisco Centralized Key Management (CCKM) fast roaming.

- When configuring WEP, there is a difference in nomenclature for the controller and the 7921 or 7920 phone. Configure the controller for 104 bits when using 128-bit WEP for the 7921 or 7920.

- For standalone 7921 phones, load-based CAC must be enabled, and the WMM Policy must be set to Required on the WLAN.

- The controller supports traffic classification (TCLAS) coming from 7921 phones using firmware version 1.1.1. This feature ensures proper classification of voice streams to the 7921 phones.

- When using a 7921 phone with the 802.11a radio of a 1242 series access point, set the 24-Mbps data rate to Supported and choose a lower Mandatory data rate (such as 12 Mbps). Otherwise, the phone might experience poor voice quality.

Using the GUI to Configure QBSS

To configure QBSS using the controller GUI, follow these steps:

**Step 1** Choose **WLANs** to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure WMM mode.

**Step 3** When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page (see Figure 7-14).
Configure WMM Mode and CAC Mode on a WLAN

Step 4 From the WMM Policy drop-down list, choose one of the following options, depending on whether you want to enable WMM mode for 7921 phones and other devices that meet the WMM standard:

- **Disabled**—Disables WMM on the WLAN. This is the default value.
- **Allowed**—Allows client devices to use WMM on the WLAN.
- **Required**—Requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

Step 5 Select the **7920 AP CAC** check box if you want to enable 7920 support mode for phones that require access point-controlled CAC. The default value is unselected.

Step 6 Select the **7920 Client CAC** check box if you want to enable 7920 support mode for phones that require client-controlled CAC. The default value is unselected.

**Note** You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your changes.

Using the CLI to Configure QBSS

To configure QBSS using the controller CLI, follow these steps:

Step 1 Determine the ID number of the WLAN to which you want to add QBSS support by entering this command:

```
show wlan summary
```

Step 2 Disable the WLAN by entering this command:

```
config wlan disable wlan_id
```

Step 3 Configure WMM mode for 7921 phones and other devices that meet the WMM standard by entering this command:

```
config wlan wmm {disabled | allowed | required} wlan_id
```

where
- **disabled** disables WMM mode on the WLAN.
• **allowed** allows client devices to use WMM on the WLAN.
• **required** requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

**Step 4**
Enable or disable 7920 support mode for phones that require client-controlled CAC by entering this command:

```shell
config wlan 7920-support client-cac-limit {enable | disable} wlan_id
```

**Note**
You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

**Step 5**
Enable or disable 7920 support mode for phones that require access point-controlled CAC by entering this command:

```shell
config wlan 7920-support ap-cac-limit {enable | disable} wlan_id
```

**Step 6**
Reenable the WLAN by entering this command:

```shell
config wlan enable wlan_id
```

**Step 7**
Save your changes by entering this command:

```shell
save config
```

**Step 8**
Verify that the WLAN is enabled and the Dot11-Phone Mode (7920) text box is configured for compact mode by entering this command:

```shell
show wlan wlan_id
```

### Configuring Media Session Snooping and Reporting

Controller software release 6.0 or later releases support Voice over IP (VoIP) Media Session Aware (MSA) snooping and reporting. This feature enables access points to detect the establishment, termination, and failure of Session Initiation Protocol (SIP) voice calls and then report them to the controller and WCS. VoIP snooping and reporting can be enabled or disabled for each WLAN.

When VoIP MSA snooping is enabled, the access point radios that advertise this WLAN look for SIP voice packets that comply with SIP RFC 3261. They do not look for non-RFC 3261-compliant SIP voice packets or Skinny Call Control Protocol (SCCP) voice packets. Any SIP packets destined to or originating from port number 5060 (the standard SIP signaling port) are considered for further inspection. The access points track when Wi-Fi Multimedia (WMM) and non-WMM clients are establishing a call, are already on an active call, or are in the process of ending a call. Upstream packet classification for both client types occurs at the access point. Downstream packet classification occurs at the controller for WMM clients and at the access point for non-WMM clients. The access points notify the controller and WCS of any major call events, such as call establishment, termination, and failure.

The controller provides detailed information for VoIP MSA calls. For failed calls, the controller generates a trap log with a timestamp and the reason for failure (in the GUI) and an error code (in the CLI) to aid in troubleshooting. For successful calls, the controller shows the number and duration of calls for usage tracking purposes. WCS displays failed VoIP call information in the Events page.

### Using the GUI to Configure Media Session Snooping

To configure media session snooping using the controller GUI, follow these steps:
Chapter 7 Configuring WLANs

**Configuring DHCP**

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure media session snooping.

**Step 3** When the WLANs > Edit page appears, choose the **Advanced** tab to open the WLANs > Edit (Advanced) page (see **Figure 7-15**).

**Figure 7-15 WLANs > Edit (Advanced) Page**

**Step 4** Under the Voice, select the **Media Session Snooping** check box to enable media session snooping or unselect it to disable this feature. The default value is unselected.

**Step 5** Click **Apply** to commit your changes.

**Step 6** Click **Save Configuration** to save your changes.

**Step 7** See the VoIP statistics for your access point radios as follows:

a. Choose **Monitor > Access Points > Radios > 802.11a/n** or **802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page.

b. Scroll to the right and click the **Detail** link for the access point for which you want to view VoIP statistics. The Radio > Statistics page appears (see **Figure 7-16**).
The VoIP Stats section shows the cumulative number and length of voice calls for this access point radio. Entries are added automatically when voice calls are successfully placed and deleted when the access point disassociates from the controller.

**Step 8** Choose **Management > SNMP > Trap Logs** to see the traps generated for failed calls. The Trap Logs page appears (Figure 7-17).

![Figure 7-17 Trap Logs Page](image)

For example, log 0 in Figure 7-17 shows that a call failed. The log provides the date and time of the call, a description of the failure, and the reason why the failure occurred.

**Using the CLI to Configure Media Session Snooping**

To configure VoIP snooping using the controller CLI, follow these steps:

**Step 1** Enable or disable VoIP snooping for a particular WLAN by entering this command:

```
config wlan call-snoop {enable | disable} wlan_id
```

**Step 2** Save your changes by entering this command:
save config

Step 3  See the status of media session snooping on a particular WLAN by entering this command:

```plaintext
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier.......................... 1
Profile Name................................ wpa2-psk
Network Name (SSID)......................... wpa2-psk
Status.................................... Enabled
...
H-REAP Local Switching..................... Disabled
H-REAP Learn IP Address.................... Enabled
Infrastructure MFP protection............ Enabled (Global Infrastructure MFP Disabled)
Client MFP................................... Optional
Tkip MIC Countermeasure Hold-down Timer... 60
Call Snooping............................. Enabled
```

Step 4  See the call information for an MSA client when media session snooping is enabled and the call is active by entering this command:

```plaintext
show call-control client callInfo client_MAC_address
```

Information similar to the following appears:

```
Uplink IP/port............................................. 192.11.1.71 / 23870
Downlink IP/port................................. 192.12.1.47 / 2070
UP....................................................... 6
Calling Party........................................ sip:1054
Called Party......................................... sip:1000
Call ID............................................... 58635b00-850161b7-14853-1501a8
Number of calls for given client is......... 1
```

Step 5  See the metrics for successful calls or the traps generated for failed calls by entering this command:

```plaintext
show call-control ap {802.11a | 802.11b} Cisco_AP {metrics | traps}
```

Information similar to the following appears when you enter `show call-control ap {802.11a | 802.11b} Cisco_AP metrics`:

```
Total Call Duration in Seconds.............. 120
Number of Calls................................... 10
```

Information similar to the following appears when you enter `show call-control ap {802.11a | 802.11b} Cisco_AP traps`:

```
Number of traps sent in one min........... 2
Last SIP error code.......................... 404
Last sent trap timestamp................... Jun 20 10:05:06
```

To aid in troubleshooting, the output of this command shows an error code for any failed calls. Table 7-3 explains the possible error codes for failed calls.

**Table 7-3 Error Codes for Failed VoIP Calls**

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Integer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>unknown</td>
<td>Unknown error.</td>
</tr>
<tr>
<td>400</td>
<td>badRequest</td>
<td>The request could not be understood because of malformed syntax.</td>
</tr>
<tr>
<td>401</td>
<td>unauthorized</td>
<td>The request requires user authentication.</td>
</tr>
</tbody>
</table>
### Table 7-3  Error Codes for Failed VoIP Calls (continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Integer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>402</td>
<td>paymentRequired</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>403</td>
<td>forbidden</td>
<td>The server understood the request but refuses to fulfill it.</td>
</tr>
<tr>
<td>404</td>
<td>notFound</td>
<td>The server has information that the user does not exist at the domain specified in the Request-URI.</td>
</tr>
<tr>
<td>405</td>
<td>methodNotAllowed</td>
<td>The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.</td>
</tr>
<tr>
<td>406</td>
<td>notAcceptable</td>
<td>The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header text box sent in the request.</td>
</tr>
<tr>
<td>407</td>
<td>proxyAuthenticationRequired</td>
<td>The client must first authenticate with the proxy.</td>
</tr>
<tr>
<td>408</td>
<td>requestTimeout</td>
<td>The server could not produce a response within a suitable amount of time, if it could not determine the location of the user in time.</td>
</tr>
<tr>
<td>409</td>
<td>conflict</td>
<td>The request could not be completed due to a conflict with the current state of the resource.</td>
</tr>
<tr>
<td>410</td>
<td>gone</td>
<td>The requested resource is no longer available at the server, and no forwarding address is known.</td>
</tr>
<tr>
<td>411</td>
<td>lengthRequired</td>
<td>The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.</td>
</tr>
<tr>
<td>413</td>
<td>requestEntityTooLarge</td>
<td>The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.</td>
</tr>
<tr>
<td>414</td>
<td>requestURITooLarge</td>
<td>The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.</td>
</tr>
<tr>
<td>415</td>
<td>unsupportedMediaType</td>
<td>The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.</td>
</tr>
<tr>
<td>420</td>
<td>badExtension</td>
<td>The server did not understand the protocol extension specified in a Proxy-Require or Require header text box.</td>
</tr>
<tr>
<td>480</td>
<td>temporarilyNotAvailable</td>
<td>The callee’s end system was contacted successfully, but the callee is currently unavailable.</td>
</tr>
<tr>
<td>481</td>
<td>callLegDoesNotExist</td>
<td>The UAS received a request that does not match any existing dialog or transaction.</td>
</tr>
<tr>
<td>482</td>
<td>loopDetected</td>
<td>The server has detected a loop.</td>
</tr>
<tr>
<td>483</td>
<td>tooManyHops</td>
<td>The server received a request that contains a Max-Forwards header text box with the value zero.</td>
</tr>
<tr>
<td>484</td>
<td>addressIncomplete</td>
<td>The server received a request with a Request-URI that was incomplete.</td>
</tr>
</tbody>
</table>
Table 7-3  Error Codes for Failed VoIP Calls (continued)

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Integer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>485</td>
<td>ambiguous</td>
<td>The Request-URI was ambiguous.</td>
</tr>
<tr>
<td>486</td>
<td>busy</td>
<td>The callee’s end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.</td>
</tr>
<tr>
<td>500</td>
<td>internalServerError</td>
<td>The server encountered an unexpected condition that prevented it from fulfilling the request.</td>
</tr>
<tr>
<td>501</td>
<td>notImplemented</td>
<td>The server does not support the functionality required to fulfill the request.</td>
</tr>
<tr>
<td>502</td>
<td>badGateway</td>
<td>The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.</td>
</tr>
<tr>
<td>503</td>
<td>serviceUnavailable</td>
<td>The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.</td>
</tr>
<tr>
<td>504</td>
<td>serverTimeout</td>
<td>The server did not receive a timely response from an external server it accessed in attempting to process the request.</td>
</tr>
<tr>
<td>505</td>
<td>versionNotSupported</td>
<td>The server does not support or refuses to support the SIP protocol version that was used in the request.</td>
</tr>
<tr>
<td>600</td>
<td>busyEverywhere</td>
<td>The callee’s end system was contacted successfully, but the callee is busy or does not want to take the call at this time.</td>
</tr>
<tr>
<td>603</td>
<td>decline</td>
<td>The callee’s machine was contacted successfully, but the user does not want to or cannot participate.</td>
</tr>
<tr>
<td>604</td>
<td>doesNotExistAnywhere</td>
<td>The server has information that the user indicated in the Request-URI does not exist anywhere.</td>
</tr>
<tr>
<td>606</td>
<td>notAcceptable</td>
<td>The user’s agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.</td>
</tr>
</tbody>
</table>

Note: If you experience any problems with media session snooping, enter the `debug call-control {all | event} {enable | disable}` command to debug all media session snooping messages or events.

Configuring Reanchoring of Roaming Voice Clients

You can allow voice clients to get anchored on the best suited and nearest available controller, which is useful when intercontroller roaming occurs. By using this feature, you can avoid the use of tunnels to carry traffic between the foreign controller and the anchor controller and remove unnecessary traffic from the network.
The ongoing call during roaming is not affected and can continue without any problem. The traffic passes through proper tunnels that are established between the foreign controller and the anchor controller. Disassociation occurs only after the call ends, and then the client then gets reassociated to a new controller.

**Note**
The ongoing data session might be affected due to disassociation and then reassociation.

**Note**
This feature is supported for TSPEC-based calls and non-TSPEC SIP-based calls only when you enable the admission control.

**Note**
You can reanchor roaming of voice clients for each WLAN.

**Note**
This feature is not recommended for use on Cisco 792x phones.

### Using the GUI to Configure Reanchoring of Roaming Voice Clients

To configure reanchoring of roaming clients using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN for which you want to configure reanchoring of roaming voice clients.

**Step 3** When the WLANs > Edit page appears, choose the Advanced tab to open the WLANs > Edit (Advanced) page (see Figure 7-18).

**Figure 7-18 WLANs > Edit (Advanced) Page**

![WLANs > Edit (Advanced) Page](image)

**Step 4** In the Voice area select the Re-anchor Roamed Clients check box.

**Step 5** Click Apply to commit your changes.
Using the CLI to Configure Reanchoring of Roaming Voice Clients

To configure reanchoring of roaming voice clients using the controller CLI, follow these steps:

**Step 1** Enable or disable reanchoring of roaming voice clients for a particular WLAN by entering this command:
```
config wlan roamed-voice-client re-anchor {enable | disable} wlan id
```

**Step 2** Save your changes by entering this command:
```
save config
```

**Step 3** See the status of reanchoring roaming voice client on a particular WLAN by entering this command:
```
show wlan wlan_id
```
Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
... Call Snooping.................................... Enabled
Roamed Call Re-Anchor Policy..................... Enabled
Band Select...................................... Disabled
Load Balancing................................... Disabled
```

**Step 4** Save your changes by entering this command:
```
save config
```

Configuring IPv6 Bridging

Internet Protocol version 6 (IPv6) is the next-generation network layer Internet protocol intended to replace version 4 (IPv4) in the TCP/IP suite of protocols. This new version increases Internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, providing significantly more addresses than the 32-bit IPv4 addresses. Follow the instructions in this section to configure a WLAN for IPv6 bridging using either the controller GUI or CLI.

**Guidelines for Using IPv6 Bridging**

Follow these guidelines when using IPv6 bridging:
- To use IPv6 bridging, multicast must be enabled on the controller.
- Hybrid-REAP with central switching is supported for use with IPv6 bridging. Hybrid-REAP with local switching is not supported.
- Auto-anchor mobility is not supported for use with IPv6 bridging.
· If symmetric mobility tunneling is enabled, all IPv4 traffic is bidirectionally tunneled to and from the client, but the IPv6 client traffic is bridged locally.

· Clients must support IPv6 with either static stateless autoconfiguration (such as Windows XP clients) or stateful DHCPv6 IP addressing (such as Windows Vista clients).

Note: Currently, DHCPv6 is supported for use only with Windows Vista clients. For these clients, you must manually renew the DHCPv6 IP address after the client changes VLANs.

Note: Dynamic VLAN function on IPv6 bridging environment is not supported on the Controller software release 6.0 and 7.0.

· For stateful DHCPv6 IP addressing to operate properly, you need a switch or router that supports the DHCP for IPv6 feature (such as the Catalyst 3750 switch) and is configured to act like a DHCPv6 server, or you need a dedicated server such as a Windows 2008 server with a built-in DHCPv6 server.

Note: To load the SDM IPv6 template in the Catalyst 3750 switch, enter the `sdm prefer dual-ipv4-and-v6 default` command and then reset the switch. For more information, see Catalyst 3750 Switch Configuration Guide for Cisco IOS Release 12.2(46)SE.

· In controller software release 4.2 or later releases, you can enable IPv6 bridging and IPv4 web authentication on the same WLAN, a combination that previously was not supported. The controller bridges IPv6 traffic from all clients on the WLAN while IPv4 traffic goes through the normal web authentication process. The controller begins bridging IPv6 as soon as the client associates and even before web authentication for IPv4 clients is complete. No other Layer 2 or Layer 3 security policy configuration is supported on the WLAN when both IPv6 bridging and web authentication are enabled. Figure 7-19 shows how IPv6 bridging and IPv4 web authentication can be used on the same WLAN.

· In controller software release 6.0 or later releases, all Layer 2 security policies are supported and can be configured when you enable IPv6 bridging on a WLAN.
Figure 7-19 IPv6 Bridging and IPv4 Web Authentication

The Security Policy Completed text box in both the controller GUI and CLI shows “No for IPv4 (bridging allowed for IPv6)” until web authentication is completed. You can view this text box from the Clients > Detail page on the GUI or from the `show client detail` CLI command.

Using the GUI to Configure IPv6 Bridging

To configure a WLAN for IPv6 bridging using the controller GUI, follow these steps:

- **Step 1** Choose WLANs to open the WLANs page.
- **Step 2** Click the ID number of the desired WLAN to open the WLANs > Edit page.
- **Step 3** Choose the Advanced tab to open the WLANs > Edit (Advanced tab) page (see Figure 7-20).
Figure 7-20 WLANs > Edit (Advanced) Page

Step 4 Select the IPv6 Enable check box if you want to enable clients that connect to this WLAN to accept IPv6 packets. Otherwise, leave the check box unselected, which is the default value.

Note If you disable (or uncheck) the IPv6 check box, IPv6 will only be allowed after authentication.

Note Enabling IPv6 means that the controller can pass IPv6 traffic without client authentication.

Step 5 Click Apply to commit your changes.

Step 6 Click Save Configuration to save your changes.

Using the CLI to Configure IPv6 Bridging

Configure a WLAN for IPv6 bridging using the controller CLI by entering this command:

```
config wlan IPv6support {enable | disable} wlan_id
```

The default value is disabled.

Configuring Cisco Client Extensions

Cisco Client Extensions (CCX) software is licensed to manufacturers and vendors of third-party client devices. The CCX code resident on these clients enables them to communicate wirelessly with Cisco access points and to support Cisco features that other client devices do not, including those features related to increased security, enhanced performance, fast roaming, and superior power management.

The 4.2 or later releases of controller software support CCX versions 1 through 5, which enables controllers and their access points to communicate wirelessly with third-party client devices that support CCX. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. However, you can configure a specific CCX feature per WLAN. This feature is Aironet information elements (IEs).
If Aironet IE support is enabled, the access point sends an Aironet IE 0x85 (which contains the access point name, load, number of associated clients, and so on) in the beacon and probe responses of this WLAN, and the controller sends Aironet IEs 0x85 and 0x95 (which contains the management IP address of the controller and the IP address of the access point) in the reassociation response if it receives Aironet IE 0x85 in the reassociation request.

Follow the instructions in this section to configure a WLAN for the CCX Aironet IE feature and to see the CCX version supported by specific client devices using either the GUI or the CLI.

Note
CCX is not supported on Cisco OEAP 600 access points and all elements related to CCX are not supported.

Note
Cisco OEAP 600 do not support Aeronet IEs.

Using the GUI to Configure CCX Aironet IEs

To configure a WLAN for CCX Aironet IEs using the controller GUI, follow these steps:

Step 1 Choose WLANs to open the WLANs page.
Step 2 Click the ID number of the desired WLAN to open the WLANs > Edit page.
Step 3 Choose the Advanced tab to open the WLANs > Edit (Advanced tab) page (see Figure 7-20).
Step 4 Select the Aironet IE check box if you want to enable support for Aironet IEs for this WLAN. Otherwise, unselect this check box. The default value is enabled (or selected).
Step 5 Click Apply to commit your changes.
Step 6 Click Save Configuration to save your changes.

Using the GUI to View a Client’s CCX Version

A client device sends its CCX version in association request packets to the access point. The controller then stores the client’s CCX version in its database and uses it to limit the features for this client. For example, if a client supports CCX version 2, the controller does not allow the client to use CCX version 4 features.

To see the CCX version supported by a particular client device using the controller GUI, follow these steps:

Step 1 Choose Monitor > Clients to open the Clients page.
Step 2 Click the MAC address of the desired client device to open the Clients > Detail page (see Figure 7-21).
### Figure 7-21  Clients > Detail Page

<table>
<thead>
<tr>
<th>Client Properties</th>
<th>AP Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>AP Address</td>
</tr>
<tr>
<td>IP Address</td>
<td>AP Name</td>
</tr>
<tr>
<td>Client Type</td>
<td>AP Type</td>
</tr>
<tr>
<td>User Name</td>
<td>WLAN Profile</td>
</tr>
<tr>
<td>Port Number</td>
<td>Status</td>
</tr>
<tr>
<td>Interface</td>
<td>Association ID</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>802.1X Authentication</td>
</tr>
<tr>
<td>CCX Version</td>
<td>Reason Code</td>
</tr>
<tr>
<td>EEE Version</td>
<td>Status Code</td>
</tr>
<tr>
<td>Mobility Role</td>
<td>CF-Pollable</td>
</tr>
<tr>
<td>Mobility Peer IP Address</td>
<td>CF-Poll Request</td>
</tr>
<tr>
<td>Policy Manager State</td>
<td>Short Preamble</td>
</tr>
<tr>
<td>Client Mode</td>
<td>CBAC</td>
</tr>
<tr>
<td>Management Frame Protection</td>
<td>Channel Agility</td>
</tr>
<tr>
<td>Security Information</td>
<td>WEP State</td>
</tr>
<tr>
<td>Security Policy Completed</td>
<td>WEP Enable</td>
</tr>
<tr>
<td>Policy Type</td>
<td>N/A</td>
</tr>
<tr>
<td>Encryption Cipher</td>
<td>WEP (40 bits)</td>
</tr>
<tr>
<td>EAP Type</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Quality of Service Properties

<table>
<thead>
<tr>
<th>WMM State</th>
<th>802.1x Tag</th>
<th>Average Data Rate</th>
<th>Burst Data Rate</th>
<th>Burst Real-Time Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>enabled</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
</tr>
<tr>
<td>Silver</td>
<td>enabled</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

### Client Statistics

<table>
<thead>
<tr>
<th>Bytes Received</th>
<th>Bytes Sent</th>
<th>Packets Received</th>
<th>Packets Sent</th>
<th>Policy Errors</th>
<th>RSSI</th>
<th>SNR</th>
<th>Sample Time</th>
<th>Excessive Retries</th>
<th>Retries</th>
<th>Success Count</th>
<th>Fail Count</th>
<th>Tx Filtered</th>
</tr>
</thead>
<tbody>
<tr>
<td>2405</td>
<td>0</td>
<td>33</td>
<td>2</td>
<td>0</td>
<td>-62</td>
<td>50</td>
<td>Wed Sep 19 01:22 2007</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The CCX Version text box shows the CCX version supported by this client device. **Not Supported** appears if the client does not support CCX.

**Step 3**  Click **Back** to return to the previous screen.
Step 4

Repeat this procedure to view the CCX version supported by any other client devices.

Using the CLI to Configure CCX Aironet IEs

Enable or disable support for Aironet IEs for a particular WLAN using the controller CLI, by entering this command:

```plaintext
config wlan ccx aironet-ie {enable | disable} wlan_id
```

The default value is enabled.

Using the CLI to View a Client’s CCX Version

See the CCX version supported by a particular client device using the controller CLI by entering this command:

```plaintext
show client detail client_mac
```

Configuring Access Point Groups

After you create up to 512 WLANs on the controller, you can selectively publish them (using access point groups) to different access points to better manage your wireless network. In a typical deployment, all users on a WLAN are mapped to a single interface on the controller. Therefore, all users associated with that WLAN are on the same subnet or VLAN. However, you can choose to distribute the load among several interfaces or to a group of users based on specific criteria such as individual departments (such as Marketing) by creating access point groups. Additionally, these access point groups can be configured in separate VLANs to simplify network administration, as shown in Figure 7-22.

---

**Note**
The required access control list (ACL) must be defined on the router that serves the VLAN or subnet.

**Note**
Multicast traffic is supported with access point group VLANs. However, if the client roams from one access point to another, the client might stop receiving multicast traffic, unless IGMP snooping is enabled.

**Note**
The OEAP 600 Series access point supports a maximum of two WLANs and one remote LAN. If you have configured more than two WLANs and one remote LAN, you can assign the 600 Series access point to an AP group. The support for two WLANs and one remote LAN still applies to the AP group. If the 600 Series OEAP is in the default group, the WLAN/remote LAN ids must be lower than 8.
Figure 7-22 Access Point Groups

In Figure 7-22, three configured dynamic interfaces are mapped to three different VLANs (VLAN 61, VLAN 62, and VLAN 63). Three access point groups are defined, and each is a member of a different VLAN, but all are members of the same SSID. A client within the wireless SSID is assigned an IP address from the VLAN subnet on which its access point is a member. For example, any user that associates with an access point that is a member of access point group VLAN 61 is assigned an IP address from that subnet.

In the example in Figure 7-22, the controller internally treats roaming between access points as a Layer 3 roaming event. In this way, WLAN clients maintain their original IP addresses.

Note
Suppose that the interface mapping for a WLAN in the AP group table is the same as the WLAN interface. If the WLAN interface is changed, the interface mapping for the WLAN in the AP group table also changes to the new WLAN interface.
Suppose that the interface mapping for a WLAN in the AP group table is different from the one defined for the WLAN. If the WLAN interface is changed, then the interface mapping for the WLAN in the AP group table does not change to the new WLAN interface.

**Note**

A controller with OfficeExtend access points in an access point group publishes up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

To configure access point groups, follow these steps:

1. Configure the appropriate dynamic interfaces and map them to the desired VLANs.
   
   For example, to implement the network in Figure 7-22, create dynamic interfaces for VLANs 61, 62, and 63 on the controller. See Chapter 3, “Configuring Ports and Interfaces,” for information on how to configure dynamic interfaces.

2. Create the access point groups. See the “Creating Access Point Groups” section on page 7-58.

3. Assign access points to the appropriate access point groups. See the “Creating Access Point Groups” section on page 7-58.

### Creating Access Point Groups

After all access points have joined the controller, you can create access point groups and assign up to 16 WLANs to each group. Each access point advertises only the enabled WLANs that belong to its access point group. The access point does not advertise disabled WLANs in its access point group or WLANs that belong to another group.

You can create up to 50 access point groups for Cisco 2100 Series Controller and controller network modules; up to 300 access point groups for Cisco 4400 Series Controllers, Cisco WiSM, and 3750G wireless LAN controller switch; and up to 500 access point groups for Cisco 5500 Series Controllers.

**Note**

All OfficeExtend access points should be in the same access point group, and that group should contain no more than 15 WLANs. A controller with OfficeExtend access points in an access point group publishes only up to 15 WLANs to each connected OfficeExtend access point because it reserves one WLAN for the personal SSID.

**Note**

If you clear the configuration on the controller, all of the access point groups disappear except for the default access point group “default-group,” which is created automatically.

### Using the GUI to Create Access Point Groups

To create an access point group using the controller GUI, follow these steps:

**Step 1** Choose WLANs > Advanced > AP Groups to open the AP Groups page (see Figure 7-23).
This page lists all the access point groups currently created on the controller. By default, all access points belong to the default access point group “default-group,” unless you assign them to other access point groups.

**Note** When you upgrade to controller software release 5.2 or later releases, the controller creates the default-group access point group and automatically populates it with the first 16 WLANs (WLANs with IDs 1 through 16, or fewer if 16 WLANs are not configured). This default group cannot be modified (you cannot add WLANs to it nor delete WLANs from it). It is dynamically updated whenever the first 16 WLANs are added or deleted. If an access point does not belong to an access point group, it is assigned to the default group and uses the WLANs in that group. If an access point joins the controller with an undefined access point group name, the access point keeps its group name but uses the WLANs in the default-group access point group.

**Step 2** Click **Add Group** to create a new access point group. The Add New AP Group section appears at the top of the page.

**Step 3** In the AP Group Name text box, enter the group’s name.

**Step 4** In the Description text box, enter the group’s description.

**Step 5** Click **Add**. The newly created access point group appears in the list of access point groups on the AP Groups page.

**Note** If you ever want to delete this group, hover your cursor over the blue drop-down arrow for the group and choose **Remove**. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0 or later releases, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases.

**Step 6** Click the name of the group to edit this new group. The AP Groups > Edit (General) page appears (see Figure 7-24).
Step 7 Change the description of this access point group by entering the new text in the AP Group Description text box and click Apply.

Step 8 Choose the WLANs tab to open the AP Groups > Edit (WLANs) page. This page lists the WLANs that are currently assigned to this access point group.

Step 9 Click Add New to assign a WLAN to this access point group. The Add New section appears at the top of the page (see Figure 7-25).

Figure 7-25 AP Groups > Edit (WLANs) Page

Step 10 From the WLAN SSID drop-down list, choose the SSID of the WLAN.

Step 11 From the Interface Name drop-down list, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable network admission control (NAC) out-of-band support.

Note The interface name in the default-group access point group matches the WLAN interface.

Step 12 Select the NAC State check box to enable NAC out-of-band support for this access point group. To disable NAC out-of-band support, leave the check box unselected, which is the default value. See the “Configuring NAC Out-of-Band Integration” section on page 7-69 for more information on NAC.

Step 13 Click Add to add this WLAN to the access point group. This WLAN appears in the list of WLANs that are assigned to this access point group.

Note If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose Remove.
Chapter 7     Configuring WLANs

Repeat Step 9 through Step 13 to add any additional WLANs to this access point group.

Choose the **APs** tab to assign access points to this access point group. The AP Groups > Edit (APs) page lists the access points that are currently assigned to this group as well as any access points that are available to be added to the group. If an access point is not currently assigned to a group, its group name appears as “default-group” (see Figure 7-26).

**Figure 7-26 AP Groups > Edit (APs) Page**

Select the check box to the left of the access point name and click **Add APs** to add an access point to this access point group. The access point now appears in the list of access points currently in this access point group.

**Note**
To select all of the available access points at once, select the **AP Name** check box. All of the access points are then selected.

**Note**
If you ever want to remove an access point from the group, select the check box to the left of the access point name and click **Remove APs**. To select all of the access points at once, select the **AP Name** check box. All of the access points are then removed from this group.

**Note**
If you ever want to change the access point group to which an access point belongs, choose **Wireless > Access Points > All APs > ap_name > Advanced** tab, choose the name of another access point group from the **AP Group Name** drop-down list, and click **Apply**.

Click **Save Configuration** to save your changes.

Using the CLI to Create Access Point Groups

To create access point groups using the controller CLI, follow these steps:

**Step 1**
Create an access point group by entering this command:

```
cfg wlan apgroup add group_name
```
Configuring DHCP

Note

To delete an access point group, enter the `config wlan apgroup delete group_name` command. An error message appears if you try to delete an access point group that is used by at least one access point. Before deleting an access point group in controller software release 6.0 or later releases, move all access points in the group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the access points in a group, enter the `show wlan apgroups` command. To move the access points to another group, enter the `config ap group-name group_name Cisco_AP` command.

Step 2
Add a description to an access point group by entering this command:

```
config wlan apgroup description group_name description
```

Step 3
Assign a WLAN to an access point group by entering this command:

```
config wlan apgroup interface-mapping add group_name wlan_id interface_name
```

Note

To remove a WLAN from an access point group, enter the `config wlan apgroup interface-mapping delete group_name wlan_id` command.

Step 4
Enable or disable NAC out-of-band support for this access point group by entering this command:

```
config wlan apgroup nac {enable | disable} group_name wlan_id
```

Step 5
Configure a WLAN radio policy on the access point group by entering this command:

```
config wlan apgroup radio-policy apgroup_name wlan-id {802.11a-only | 802.11bg | 802.11g-only | all}
```

Step 6
Assign an access point to an access point group by entering this command:

```
config ap group-name group_name Cisco_AP
```

Note

To remove an access point from an access point group, reenter this command and assign the access point to another group.

Step 7
Save your changes by entering this command:

```
save config
```

Using the CLI to View Access Point Groups

To view information about or to troubleshoot access point groups, use these commands:

- See a list of all access point groups on the controller by entering this command:

```
show wlan apgroups
```

Information similar to the following appears:

```
Site Name................................. AP2
Site Description............................ Access Point 2

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Interface</th>
<th>Network Admission Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>management</td>
<td>Disabled</td>
</tr>
<tr>
<td>2</td>
<td>management</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
```
Chapter 7 Configuring WLANs

### Configuring DHCP

<table>
<thead>
<tr>
<th>AP Name</th>
<th>Slots</th>
<th>AP Model</th>
<th>Ethernet MAC</th>
<th>Location</th>
<th>Port</th>
<th>Country</th>
<th>Priority</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP1242</td>
<td>2</td>
<td>AP1242AG-A-K9</td>
<td>00:14:1c:ed:23:9a</td>
<td>default</td>
<td>1</td>
<td>US</td>
<td>1</td>
<td>AP2</td>
</tr>
</tbody>
</table>

- See the BSSIDs for each WLAN assigned to an access point group by entering this command:

  ```
  show ap wlan {802.11a | 802.11b} Cisco_AP
  ```

  Information similar to the following appears:

  ```
  Site Name........................................ AP3
  Site Description................................. Access Point 3
  ```

<table>
<thead>
<tr>
<th>WLAN ID</th>
<th>Interface</th>
<th>BSSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>management</td>
<td>00:14:1b:58:14:df</td>
</tr>
</tbody>
</table>

- See the number of WLANs enabled for an access point group by entering this command:

  ```
  show ap config {802.11a | 802.11b} Cisco_AP
  ```

  Information similar to the following appears:

  ```
  Cisco AP Identifier.............................. 166
  Cisco AP Name..................................... AP2
  ```

  ```
  Station Configuration
  Configuration ..................................... AUTOMATIC
  Number Of WLANs .................................. 2
  ```

- Enable or disable debugging of access point groups by entering this command:

  ```
  debug group {enable | disable}
  ```

### Configuring Web Redirect with 802.1X Authentication

You can configure a WLAN to redirect a user to a particular web page after 802.1X authentication has completed successfully. You can configure the web redirect to give the user partial or full access to the network.

### Conditional Web Redirect

If you enable conditional web redirect, the user can be conditionally redirected to a particular web page after 802.1X authentication has completed successfully. You can specify the redirect page and the conditions under which the redirect occurs on your RADIUS server. Conditions might include the user’s password reaching expiration or the user needing to pay his or her bill for continued usage.
Configuring DHCP

If the RADIUS server returns the Cisco AV-pair “url-redirect,” then the user is redirected to the specified URL upon opening a browser. If the server also returns the Cisco AV-pair “url-redirect-acl,” the specified access control list (ACL) is installed as a preauthentication ACL for this client. The client is not considered fully authorized at this point and can only pass traffic allowed by the preauthentication ACL.

After the client completes a particular operation at the specified URL (for example, changing a password or paying a bill), the client must reauthenticate. When the RADIUS server does not return a “url-redirect,” the client is considered fully authorized and allowed to pass traffic.

Note

The conditional web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security.

After you configure the RADIUS server, you can then configure the conditional web redirect on the controller using either the controller GUI or CLI.

Splash Page Web Redirect

If you enable splash page web redirect, the user is redirected to a particular web page after 802.1X authentication has completed successfully. After the redirect, the user has full access to the network. You can specify the redirect page on your RADIUS server. If the RADIUS server returns the Cisco AV-pair “url-redirect,” then the user is redirected to the specified URL upon opening a browser. The client is considered fully authorized at this point and is allowed to pass traffic, even if the RADIUS server does not return a “url-redirect.”

Note

The splash page web redirect feature is available only for WLANs that are configured for 802.1X or WPA+WPA2 Layer 2 security with 802.1x key management. Preshared key management is not supported with any Layer 2 security method.

After you configure the RADIUS server, you can then configure the splash page web redirect on the controller using either the controller GUI or CLI.

Using the GUI to Configure the RADIUS Server

To configure your RADIUS server using the controller GUI, follow these steps:

Note

These instructions are specific to the CiscoSecure ACS; however, they should be similar to those for other RADIUS servers.

Step 1 From the CiscoSecure ACS main menu, choose Group Setup.
Step 2 Click Edit Settings.
Step 3 From the Jump To drop-down list, choose RADIUS (Cisco IOS/PIX 6.0). The dialog box shown in Figure 7-27 appears.
Figure 7-27 ACS Server Configuration

Step 4
Select the [009\001] cisco-av-pair check box.

Step 5
Enter the following Cisco AV-pairs in the [009\001] cisco-av-pair edit box to specify the URL to which the user is redirected and, if configuring conditional web redirect, the conditions under which the redirect takes place, respectively:

url-redirect=http://url
url-redirect-acl=acl_name

Using the GUI to Configure Web Redirect

To configure conditional or splash page web redirect using the controller GUI, follow these steps:

Step 1
Choose WLANs to open the WLANs page.

Step 2
Click the ID number of the desired WLAN. The WLANs > Edit page appears.

Step 3
Choose the Security and Layer 2 tabs to open the WLANs > Edit (Security > Layer 2) page.
Step 4 From the Layer 2 Security drop-down list, choose 802.1X or WPA+WPA2.
Step 5 Set any additional parameters for 802.1X or WPA+WPA2.
Step 6 Choose the Layer 3 tab to open the WLANs > Edit (Security > Layer 3) page (see Figure 7-28).

Figure 7-28 WLANs > Edit (Security > Layer 3) Page

Step 7 From the Layer 3 Security drop-down list, choose None.
Step 8 Check the Web Policy check box.
Step 9 Choose one of the following options to enable conditional or splash page web redirect: Conditional Web Redirect or Splash Page Web Redirect. The default value is disabled for both parameters.
Step 10 If the user is to be redirected to a site external to the controller, choose the ACL that was configured on your RADIUS server from the Preauthentication ACL drop-down list.
Step 11 Click Apply to commit your changes.
Step 12 Click Save Configuration to save your changes.

Using the CLI to Configure Web Redirect

To configure conditional or splash page web redirect using the controller CLI, follow these steps:

Step 1 Enable or disable conditional web redirect by entering this command:
```bash
cfg wlan security cond-web-redir {enable | disable} wlan_id
```
Step 2 Enable or disable splash page web redirect by entering this command:
```bash
cfg wlan security splash-page-web-redir {enable | disable} wlan_id
```
Step 3 Save your settings by entering this command:
```bash
save config
```
Step 4 See the status of the web redirect features for a particular WLAN by entering this command:
```bash
show wlan wlan_id
```
Information similar to the following appears:
Using the GUI to Disable the Accounting Servers per WLAN

This section provides instructions for disabling all accounting servers on a WLAN. Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

To disable all accounting servers for a RADIUS authentication server using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the ID number of the WLAN to be modified. The WLANs > Edit page appears.

**Step 3** Choose the Security and AAA Servers tabs to open the WLANs > Edit (Security > AAA Servers) page (see Figure 7-29).

![Figure 7-29 WLANs > Edit (Security > AAA Servers) Page](image-url)
Disabling Coverage Hole Detection per WLAN

This section provides instructions for disabling coverage hole detection on a WLAN.

Coverage hole detection is enabled globally on the controller. See the “Coverage Hole Detection and Correction” section on page 12-4 and the “Using the GUI to Configure Coverage Hole Detection” section on page 12-20 for more information.

In software release 5.2 or later releases, you can disable coverage hole detection on a per-WLAN basis. When you disable coverage hole detection on a WLAN, a coverage hole alert is still sent to the controller, but no other processing is done to mitigate the coverage hole. This feature is useful for guest WLANs where guests are connected to your network for short periods of time and are likely to be highly mobile.

Using the GUI to Disable Coverage Hole Detection on a WLAN

To disable coverage hole detection on a WLAN using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

**Step 2** Click the profile name of the WLAN to be modified. The WLANs > Edit page appears.

**Step 3** Choose the Advanced tab to display the WLANs > Edit (Advanced) page (see Figure 7-30).

**Step 4** Unselect the Coverage Hole Detection Enabled check box.
Using the CLI to Disable Coverage Hole Detection on a WLAN

To disable coverage hole detection on a WLAN using the controller CLI, follow these steps:

Step 1
Disable coverage hole detection on a WLAN by entering this command:

```
config wlan chd wlan_id disable
```

**Note**
OEAP 600 Series Access Points do not support Coverage Hole detection.

Step 2
Save your settings by entering this command:

```
save config
```

Step 3
See the coverage hole detection status for a particular WLAN by entering this command:

```
show wlan wlan_id
```

Information similar to the following appears:

```
WLAN Identifier......................... 2
Profile Name.............................. wlan2
Network Name (SSID)...................... 2
.
CHD per WLAN............................. Disabled
```

Configuring NAC Out-of-Band Integration

The Cisco NAC Appliance, also known as Cisco Clean Access (CCA), is a network admission control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

In controller software releases prior to 5.1, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In controller software release 5.1 or later releases, the controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.
To implement the NAC out-of-band feature on the controller, you must enable NAC support on the WLAN or guest LAN and then map this WLAN or guest LAN to an interface that is configured with a quarantine VLAN (untrusted VLAN) and an access VLAN (trusted VLAN). When a client associates and completes Layer 2 authentication, the client obtains an IP address from the access VLAN subnet, but the client state is Quarantine. While deploying the NAC out-of-band feature, be sure that the quarantine VLAN is allowed only between the Layer 2 switch on which the controller is connected and the NAC appliance and that the NAC appliance is configured with a unique quarantine-to-access VLAN mapping. Client traffic passes into the quarantine VLAN, which is trunked to the NAC appliance. After posture validation is completed, the client is prompted to take action for remediation. After cleaning is completed, the NAC appliance updates the controller to change the client state from Quarantine to Access. Figure 7-31 provides an example of NAC out-of-band integration.

In Figure 7-31, the link between the controller and the switch is configured as a trunk, enabling the quarantine VLAN (110) and the access VLAN (10). On the Layer 2 switch, the quarantine traffic is trunked to the NAC appliance while the access VLAN traffic goes directly to the Layer 3 switch. Traffic that reaches the quarantine VLAN on the NAC appliance is mapped to the access VLAN based on a static mapping configuration.

Follow the instructions in this section to configure NAC out-of-band integration using either the controller GUI or CLI.

**Guidelines for Using NAC Out-of-Band Integration**

Follow these guidelines when using NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Multiple NAC appliances might need to be deployed.
- CCA software release 4.5 or later releases is required for NAC out-of-band integration.
- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.

When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.

NAC out-of-band integration is supported only on WLANs configured for hybrid-REAP central switching. It is not supported for use on WLANs configured for hybrid-REAP local switching.

---

**Note**  See Chapter 15, “Configuring Hybrid REAP,” for more information on hybrid REAP.

---

If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.

NAC out-of-band integration is not supported for use with the WLAN AAA override feature.

All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

---


---

### Using the GUI to Configure NAC Out-of-Band Integration

To configure NAC out-of-band integration using the controller GUI, follow these steps:

**Step 1** Configure the quarantine VLAN for a dynamic interface as follows:

- **a.** Choose **Controller > Interfaces** to open the Interfaces page.
- **b.** Click **New** to create a new dynamic interface.
- **c.** In the Interface Name text box, enter a name for this interface, such as “quarantine.”
- **d.** In the VLAN ID text box, enter a nonzero value for the access VLAN ID, such as “10.”
- **e.** Click **Apply** to commit your changes. The Interfaces > Edit page appears (see Figure 7-32).
f. Select the **Quarantine** check box and enter a nonzero value for the quarantine VLAN ID, such as “110.”

**Note** We recommend that you configure unique quarantine VLANs throughout your network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in the same subnet, it is mandatory to have the same quarantine VLAN if there is only one NAC appliance in the network. If multiple controllers are configured in the same mobility group and access interfaces on all controllers are in different subnets, it is mandatory to have different quarantine VLANs if there is only one NAC appliance in the network.

g. Configure any remaining text boxes for this interface, such as the IP address, netmask, and default gateway.

h. Click **Apply** to save your changes.

**Step 2** Configure NAC out-of-band support on a WLAN or guest LAN as follows:

a. Choose **WLANs** to open the WLANs page.

b. Click the ID number of the desired WLAN or guest LAN. The WLANs > Edit page appears.

c. Choose the **Advanced** tab to open the WLANs > Edit (Advanced) page (see Figure 7-33).
d. Configure NAC out-of-band support for this WLAN or guest LAN by selecting the **NAC State** check box. To disable NAC out-of-band support, leave the check box unselected, which is the default value.

e. Click **Apply** to commit your changes.

**Step 3** Configure NAC out-of-band support for a specific access point group as follows:

a. Choose **WLANs > Advanced > AP Groups** to open the AP Groups page (see Figure 7-34).

**Figure 7-34  AP Groups Page**

b. Click the name of the desired access point group.

c. Choose the **WLANs** tab to open the AP Groups > Edit (WLANs) page.

d. Click **Add New** to assign a WLAN to this access point group. The Add New section appears at the top of the page (see Figure 7-35).
e. From the WLAN SSID drop-down list, choose the SSID of the WLAN.

f. From the Interface Name drop-down list, choose the interface to which you want to map the access point group. Choose the quarantine VLAN if you plan to enable NAC out-of-band support.

g. To enable NAC out-of-band support for this access point group, select the NAC State check box. To disable NAC out-of-band support, leave the check box unselected, which is the default value.

h. Click Add to add this WLAN to the access point group. This WLAN appears in the list of WLANs assigned to this access point group.

**Note**  If you ever want to remove this WLAN from the access point group, hover your cursor over the blue drop-down arrow for the WLAN and choose Remove.

---

**Step 4**  Click **Save Configuration** to save your changes.

**Step 5**  See the current state of the client (Quarantine or Access) as follows:

a. Choose **Monitor > Clients** to open the Clients page.

b. Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears under the Security Information section.

**Note**  The client state appears as “Invalid” if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.

---

**Using the CLI to Configure NAC Out-of-Band Integration**

To configure NAC out-of-band integration using the controller CLI, follow these steps:

**Step 1**  Configure the quarantine VLAN for a dynamic interface by entering this command:

```
config interface quarantine vlan interface_name vlan_id
```

**Note**  You must configure a unique quarantine VLAN for each interface on the controller.
Note  To disable the quarantine VLAN on an interface, enter 0 for the VLAN ID.

Step 2  Enable or disable NAC out-of-band support for a WLAN or guest LAN by entering this command:

```
config {wlan | guest-lan} nac {enable | disable} {wlan_id | guest_lan_id}
```

Step 3  Enable or disable NAC out-of-band support for a specific access point group by entering this command:

```
config wlan apgroup nac {enable | disable} group_name wlan_id
```

Step 4  Save your changes by entering this command:

```
save config
```

Step 5  See the configuration of a WLAN or guest LAN, including the NAC state by entering this command:

```
show {wlan wlan_id | guest-lan guest_lan_id}
```

Information similar to the following appears:

```
WLAN Identifier.......................... 1
Profile Name................................. wlan
Network Name (SSID)....................... wlan
Status....................................... Disabled
MAC Filtering................................ Disabled
Broadcast SSID............................. Enabled
AAA Policy Override....................... Disabled
Network Admission Control

   NAC-State.................................. Enabled
   Quarantine VLAN.......................... 110
   ...
```

Step 6  See the current state of the client (either Quarantine or Access) by entering this command:

```
show client detailed client_mac
```

Information similar to the following appears:

```
Client's NAC state......................... QUARANTINE
```

Note  The client state appears as “Invalid” if the client is probing, has not yet associated to a WLAN, or cannot complete Layer 2 authentication.

---

**Configuring Passive Client**

Note  The passive client feature is supported on Cisco 5500 and Cisco 2100 Series Controllers.

Note  The passive client feature is not supported with the AP groups and hybrid REAP centrally switched WLANs.
The passive client feature works in multicast-multicast and multicast-unicast mode. The controller sources the multicast packets using its management IP address.

Passive clients are wireless devices, such as scales and printers that are configured with a static IP address. These clients do not transmit any IP information such as IP address, subnet mask, and gateway information when they associate with an access point. As a result, when passive clients are used, the controller never knows the IP address unless they use the DHCP.

Wireless LAN controllers currently act as a proxy for ARP requests. Upon receiving an ARP request, the controller responds with an ARP response instead of passing the request directly to the client. This scenario has two advantages:

- The upstream device that sends out the ARP request to the client will not know where the client is located.
- Power for battery-operated devices such as mobile phones and printers is preserved because they do not have to respond to every ARP requests.

Since the wireless controller does not have any IP related information about passive clients, it cannot respond to any ARP requests. The current behavior does not allow the transfer of ARP requests to passive clients. Any application that tries to access a passive client will fail.

The passive client feature enables the ARP requests and responses to be exchanged between wired and wireless clients. This feature when enabled, allows the controller to pass ARP requests from wired to wireless clients until the desired wireless client gets to the RUN state.

**Using the GUI to Configure Passive Client**

This section describes how to configure passive client using the controller GUI.

**Enabling the Multicast-Multicast Mode**

To enable the multicast-multicast mode, follow these steps:

**Step 1** Choose Controller > General to open the General page. See Figure 7-36.
Figure 7-36  Controller > General Page

Step 2 Choose one of the following options from the AP Multicast Mode drop-down list:

- **Unicast**—Configures the controller to use the unicast method to send multicast packets. This is the default value.

- **Multicast**—Configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

Step 3 Select Multicast from the AP Multicast Mode drop-down list. The Multicast Group Address text box is displayed.

Step 4 In the Multicast Group Address text box, enter the IP address of the multicast group.

Step 5 Click **Apply** to commit your changes.

Step 6 Click Multicast to enable the global multicast mode (see Figure 7-37).

---

Enabling the Global Multicast Mode on Controllers

To enable the global multicast mode, follow these steps:

Step 1 Choose Controller > **Multicast** to open the Multicast page (see Figure 7-37.)
Figure 7-37  Multicast Page

The Enable IGMP Snooping text box is highlighted only when you enable the Enable Global Multicast mode. The IGMP Timeout (seconds) text box is highlighted only when you enable the Enable IGMP Snooping text box.

Step 2  Select the **Enable Global Multicast Mode** check box to enable the multicast mode. This step configures the controller to use the multicast method to send multicast packets to a CAPWAP multicast group.

Step 3  Select the **Enable IGMP Snooping** check box to enable the IGMP snooping. The default value is disabled.

Step 4  In the IGMP Timeout text box to set the IGMP timeout, enter a value between 30 and 7200 seconds.

Step 5  Click **Apply** to commit your changes.

Enabling the Passive Client Feature on the Controller

To enable the passive client feature on the controller, follow these steps:

Step 1  Choose WLANs > WLANs > WLAN ID to open the WLANs > Edit page (see Figure 7-38). By default, the General tab is displayed.

Step 2  Choose the **Advanced** tab.
Step 3  Select the **Passive Client** check box (see Figure 7-39) to enable the passive client feature.

![Figure 7-39 WLAN > Edit > Advanced Tab Page](image)

Step 4  Click **Apply** to commit your changes.

**Using the CLI to Configure Passive Client**

To configure passive client using the controller CLI, follow these steps:

**Note**  Make sure that you enable the multicast mode before you configure the passive client feature.

Step 1  Enable or disable multicasting on the controller by entering this command:

```
config network multicast global { enable | disable }
```

The default value is disabled.

Step 2  Configure the controller to use multicast to send multicast to an access point by entering this command:
config network multicast mode multicast multicast_group_IP_address

Step 3 Configure passive client on a wireless LAN by entering this command:

config wlan passive-client {enable | disable} wlan_id

Step 4 Configure a WLAN by entering this command:

config wlan

Step 5 Save your changes by entering this command:

save config

Step 6 Display the passive client information on a particular WLAN by entering this command:

show wlan

Information similar to the following appears:

WLAN Identifier.................................. 2
Profile Name.................................... passive
Network Name (SSID).............................. passive
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID.................................. Enabled
AAA Policy Override............................. Disabled
Network Admission Control
   MAC-Admission Control.................... Disabled
   Quarantine VLAN............................. 0
Number of Active Clients...................... 1
Exclusionlist Timeout.......................... 60 seconds
Session Timeout............................... 1800 seconds
CHD per WLAN.................................. Enabled
Webauth DHCP exclusion....................... Disabled
Interface....................................... management
WLAN ACL....................................... unconfigured
DHCP Server.................................... Default
DHCP Address Assignment Required........... Disabled
--More-- or (q)uit
Quality of Service............................. Silver (best effort)
WMM............................................... Allowed
CCX - Aironet Support......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)........ Disabled
CCX - Diagnostics Channel Capability........ Disabled
Dot11-Phone Mode (7920)....................... Disabled
Wired Protocol.................................. None
IPv6 Support.................................... Disabled
Passive Client Feature......................... Enabled
Peer-to-Peer Blocking Action................... Disabled
Radio Policy.................................... All
DTIM period for 802.11a radio.................. 1
DTIM period for 802.11b radio.................. 1
Radius Servers
   Authentication................................ Global Servers
   Accounting.................................... Global Servers
Local EAP Authentication...................... Disabled
Security
   802.11 Authentication:..................... Open System
   Static WEP Keys............................. Disabled
   802.1X........................................ Disabled
   WPA-Protected Access (WPA/WPA2)........... Disabled
--More-- or (q)uit
   CKIP.......................................... Disabled
   Web Based Authentication................... Disabled
   Web-Passthrough............................ Disabled
   Conditional Web Redirect................... Disabled
Splash-Page Web Redirect......................... Disabled
Auto Anchor.................................... Disabled
H-REAP Local Switching......................... Disabled
H-REAP Learn IP Address......................... Enabled
Infrastructure MFP protection............... Enabled (Global Infrastructure MFP Disabled)
Client MFP..................................... Optional but inactive (WPA2 not configured)
Tkip MIC Countermeasure Hold-down Timer....... 60
Call Snooping.................................... Disabled
Band Select...................................... Enabled
Load Balancing................................... Enabled

Step 7 Verify if the passive client is associated correctly with the AP and if the passive client has moved into the DHCP required state at the controller by entering this command:

debug client mac_address

Step 8 Display the detailed information for a client by entering this command:

show client detail mac_address

Information similar to the following appears:

Client MAC Address............................... 00:0d:28:f4:c0:45
Client Username ................................. N/A
AP MAC Address.................................. 00:14:1b:58:19:00
Client State..................................... Connected
Client NAC OOB State............................ Access
Wireless LAN Id.................................. 1
BSSID............................................... 00:14:1b:58:19:00
Connected For ................................... 8 secs
Channel............................................ 11
IP Address....................................... Unknown

Security Policy Completed....................... No
Policy Manager State............................. DHCP_REQD
Policy Manager Rule Created.................... Yes
ACL Name........................................ none
ACL Applied Status............................ Unavailable

Step 9 Check if the client moves into the run state, when a wired client tries to contact the client by entering this command:

debug client mac_address

Step 10 Configure and check if the arp request is forwarded from the wired side to the wireless side by entering this command:

debug arp all enable

Information similar to the following appears:

*dtlArpTask: Apr 15 10:54:26.161: Received dtlArpRequest
  sha: 00:19:06:61:b1:c3 spa: 80.4.1.1
  tha: 00:00:00:00:00:00 tpa: 80.4.0.50
  intf: 1, vlan: 71, node type: 1, mscb: not found, isFromSta: 0^M^M
*dtlArpTask: Apr 15 10:54:26.161: dtlArpFindClient:ARP look-up for 80.4.0.50 failed (not a client).

*dtlArpTask: Apr 15 10:54:26.161: Dropping ARP to DS (mscb (nil), port 65535)
  sha 0019.0661.b1c3 spa: 80.4.1.1
  tha 0000.0000.0000 tpa: 80.4.0.50
*dtlArpTask: Apr 15 10:54:26.161: Arp from Wired side to passive client
Per-WLAN RADIUS Source Support

By default, the controller sources all RADIUS traffic from the IP address on its management interface. This means that even if a WLAN has specific RADIUS servers configured instead of the global list, the identity used is the management interface IP address.

If you want to do a per-user WLAN filtering, you can use the callStationID set by RFC 3580 to be in the APMAC:SSID format. You can also extend the filtering on the authentication server to be on a per-WLAN source interface by using the NAS-IP-Address attribute.

When the per-WLAN RADIUS source support is enabled, the controller sources all RADIUS traffic for a particular WLAN using the dynamic interface that is configured. Also, RADIUS attributes are modified accordingly to match the identity. This feature effectively virtualizes the controller on the per-WLAN RADIUS traffic, where each WLAN can have a separate L3 identity. This feature is useful in ACS Network Access Restrictions, Network Access Profiles, and so on.

This feature can be combined with normal RADIUS traffic source, with some WLANs using the management interface and others using the per-WLAN dynamic interface as the address source.

Configuring Per-WLAN RADIUS Source Support

You can configure the per-WLAN RADIUS source support using only the controller CLI:

Step 1  Enter the `config wlan disable wlan-id` command to disable the WLAN.

Step 2  Enter the following command to enable or disable the per-WLAN RADIUS source support:

```
config wlan radius_server overwrite-interface {enable | disable} wlan-id
```

Note When enabled, the controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on that WLAN.

When disabled, the controller uses the management interface as the identity in the NAS-IP-Address attribute. If the RADIUS server is on a directly connected dynamic interface, the RADIUS traffic will be sourced from that interface. Otherwise, the management IP address is used. In all cases, the NAS-IP-Address attribute remains the management interface, unless the feature is enabled.

Step 3  Enter the `config wlan enable wlan-id` command to enable the WLAN.

Note You can filter requests on the RADIUS server side using CiscoSecure ACS. You can filter (accept or reject) a request depending on the NAS-IP-Address attribute through a Network Access Restrictions rule. The filtering to be used is the CLI/DNIS filtering.
Monitoring the Status of Per-WLAN RADIUS Source Support

To see if the feature is enabled or disabled, enter the following command:

```
show wlan wlan-id
```

**Example**

The following example shows that the per-WLAN RADIUS source support is enabled on WLAN 1.

```
show wlan /
```

Information similar to the following is displayed:

```
WLAN Identifier.................. 4
Profile Name...................... 4400-wpa2
Network Name (SSID)............. 4400-wpa2
Status............................. Enabled
MAC Filtering..................... Disabled
Broadcast SSID.................... Enabled
AAA Policy Override.............. Disabled
Network Admission Control

... Radius Servers
   Authentication.................. Global Servers
   Accounting...................... Global Servers
   Overwrite Sending Interface.... Enabled
   Local EAP Authentication........ Disabled
```

**Guidelines and Limitations**

- It is up to the authentication server (RADIUS) to implement a proper rule filtering on the new identity because the controller sources traffic only from the selected interface.
- callStationID is always in the APMAC:SSID format to comply with 802.1x over RADIUS RFC. This is also a legacy behavior. Web-auth can use different formats available in the `config radius callStationIDType` command.
- If AP groups or AAA override are used, the source interface remains the WLAN interface, and not what is specified on the new AP group or RADIUS profile configuration.

**Configuring Remote LANs**

This section describes how to configure remote LANs using the controller GUI and CLI.

---

**Caution**

You must remove all remote LANs from a controller's configuration before moving to a release that does not support the remote LAN functionality. The remote LAN changes to a WLAN in earlier releases, which could cause an undesirable or unsecured WLAN being broadcast on the wireless network. Remote LAN is only supported in release 7.0.116.0 and later.

---

**Note**

Only four clients can connect to an OEAP 600 series access point through a remote LAN port. This number does not affect the fifteen WLAN limit imposed for the controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.
Note: Remote LAN can be applied on a dedicated LAN port on an OEAP 600 series access point.

Using the GUI to Configure a Remote LAN

To create remote LANs using the controller GUI, follow these steps:

**Step 1** Choose WLANs to open the WLANs page.

This page lists all of the WLANs and remote LANs currently configured on the controller. For each WLAN, you can see its WLAN/remote LAN ID, profile name, type, SSID, status, and security policies.

The total number of WLANs/Remote LANs appears in the upper right-hand corner of the page. If the list of WLANs/Remote LANs spans multiple pages, you can access these pages by clicking the page number links.

Note: If you want to delete a Remote LAN, hover your cursor over the blue drop-down arrow for that WLAN and choose **Remove**, or select the check box to the left of the row, choose **Remove Selected** from the drop-down list, and click **Go**. A message appears asking you to confirm your decision. If you proceed, the remote LAN is removed from any access point group to which it is assigned and from the access point's radio.

**Step 2** Create a new Remote-LAN by choosing **Create New** from the drop-down list and clicking **Go**. The WLANs > New page appears.

**Step 3** From the Type drop-down list, choose **Remote LAN** to create a remote LAN.

**Step 4** In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this Remote WLAN. The profile name must be unique.

**Step 5** From the WLAN ID drop-down list, choose the ID number for this WLAN.

**Step 6** Click **Apply** to commit your changes. The WLANs > Edit page appears (see Figure 7-3).

Note: You can also open the WLANs > Edit page from the WLANs page by clicking the ID number of the WLAN that you want to edit.

**Step 7** Use the parameters on the General, Security, and Advanced tabs to configure this remote LAN. See the sections in the rest of this chapter for instructions on configuring specific features.

**Step 8** On the General tab, select the **Status** check box to enable this remote LAN. Be sure to leave it unselected until you have finished making configuration changes to the remote LAN.

Note: You can also enable or disable remote LANs from the WLANs page by selecting the check boxes to the left of the IDs that you want to enable or disable, choosing **Enable Selected** or **Disable Selected** from the drop-down list, and clicking **Go**.

**Step 9** Click **Apply** to commit your changes.

**Step 10** Click **Save Configuration** to save your changes.
Using the CLI to Configure a Remote LAN

To configure 802.1X for a remote LAN using the controller CLI, use the following commands:

- See the current configuration of the remote LAN by entering this command:
  
  `show remote-lan remote-lan-id`

- Enable or disable remote LAN by entering this command:
  
  `config remote-lan {enable | disable} remote-lan-id`

- Enable or disable 802.1X authentication for remote LAN by entering this command:
  
  `config remote-lan security 802.1X {enable | disable} remote-lan-id`

**Caution**

The 802.1x authentication settings for a Remote LAN can only be configured or modified using the controller CLI. If a remote LAN is accessed through the controller GUI and any configuration changes are performed; regardless of any modifications from the GUI; the 802.1x settings for that remote LAN will be removed and whatever settings are shown in the GUI will be applied.

**Note**

The encryption on a remote LAN is always “none”.

- Enable or disable local EAP with the controller as an authentication server, by entering this command:
  
  `config remote-lan local-auth enable profile-name remote-lan-id`

- If you are using an external AAA authentication server, use the following command:
  
  `config remote-lan radius_server auth {add | delete} remote-lan-id server id`

  `config remote-lan radius_server auth {enable | disable} remote-lan-id`