WLANs

Information About WLANs

This feature enables you to control up to WLANs for lightweight access points. Each WLAN has a separate WLAN ID, 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 the maximum number of WLANs supported and then selectively publish these WLANs (using access point groups) to different access points to better manage your wireless network.

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

Guidelines and Limitations

Creating WLANs

Creating and Removing WLANs (GUI)

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

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 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**.

Step 4 In the Profile Name text box, enter up to 32 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 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.

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.

Step 10 Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Enabling and Disabling WLANs (GUI)

Step 1 Choose **WLANs** to open the WLANs page.
This page lists all of the WLANs currently configured on the controller.

Step 2 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 3 Click **Apply**.

Creating and Deleting WLANs (CLI)

- 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.

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.

- 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.

- View the WLANs configured on the controller by entering this command:

  show wlan summary

Enabling and Disabling WLANs (CLI)

- 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").

- 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.

Note If the WLAN is disabled, the VLAN acls corresponding to the WLAN-VLAN mapping at the AP is pushed to the AP and has precedence over the group mappings. Before WLAN is disabled there should be 16 sub interface created for vlan-acl mapping and 3 ap specific WLAN-VLAN mapping and 3 more sub interface should be created for group specific WLAN-VLAN mapping, as of now out of 16 vlan-acl mapping only 14 are pushed. After disabling all the WLAN only vlan-acl sub interface should be pushed and other sub interface should be deleted from the AP.

Viewing WLANs (CLI)

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

  show wlan summary

Searching WLANs (GUI)

Step 1 On the WLANs page, click **Change Filter**. The Search WLANs dialog box appears.

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**.

Setting the Client Count per WLAN

Information About Setting the Client Count 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 for each WLAN depends on the platform that you are using.

Guidelines and Limitations

- The maximum number of clients for each WLAN feature is not supported when you use FlexConnect local authentication.
- The maximum number of clients for each WLAN feature is supported only for access points that are in connected mode.
- When a WLAN has reached the limit on the maximum number of clients connected to it or an AP radio and a new client tries to join the WLAN, the client cannot connect to the WLAN until an existing client gets disconnected.
- Roaming clients are considered as new clients. The new client can connect to a WLAN, which has reached the maximum limit on the number of connected clients, only when an existing client gets disconnected.

Note For more information about the number of clients that are supported, see the product data sheet of your controller.

Configuring the Client Count per WLAN (GUI)

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 Click the **Advanced** tab.

Step 4 In the **Maximum Allowed Clients** text box, enter the maximum number of clients that are to be allowed.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring the Maximum Number of Clients per WLAN (CLI)

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

Get the WLAN ID from the list.

Step 2 Configure the maximum number of clients for each WLAN by entering this command:
config wlan max-associated-clients *max-clients wlan-id*

Configuring the Maximum Number of Clients for each AP Radio per WLAN (GUI)

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 In the **Advanced** tab, enter the maximum allowed clients for each access point radio in the Maximum Allowed Clients Per AP Radio text box. You can configure up to 200 clients.

Step 4 Click **Apply**.

Configuring the Maximum Number of Clients for each AP Radio per WLAN (CLI)

Step 1 Determine the WLAN ID for which you want to configure the maximum clients for each radio by entering this command: **show wlan summary**

Obtain the WLAN ID from the list.

Step 2 Configure the maximum number of clients for each WLAN by entering this command: **config wlan max-radio-clients** *client_count*

You can configure up to 200 clients.

Step 3 See the configured maximum associated clients by entering the **show 802.11a** command.

Configuring DHCP

Information About the Dynamic Host Configuration Protocol

You can configure WLANs 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 Servers

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 a maximum of 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, 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, Domain Name System (DNS), or priming.

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

When clients use the internal DHCP server of the controller, IP addresses are not preserved across reboots. As a result, multiple clients can be assigned with the same IP address. To resolve any IP address conflicts, clients must release their existing IP address and request a new one. Wired guest clients are always on a Layer 2 network connected to a local or foreign controller.

Note DHCPv6 is not supported in the internal DHCP servers.

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

Note External DHCP servers can support DHCPv6.

DHCP Assignments

You can configure DHCP on a per-interface or per-WLAN basis. We recommend that you use the primary DHCP server address that is assigned to a particular interface.

You can assign DHCP servers for individual interfaces. You can configure the management interface, AP-manager interface, and dynamic interface for a primary and secondary DHCP server, and you can configure the service-port interface to enable or disable DHCP servers. You can also define a DHCP server on a WLAN. In this case, the server overrides 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, you can configure all WLANs 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 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.

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 can create separate WLANs with DHCP Addr. Assignment Required configured as disabled. This is applicable only if DHCP proxy is enabled for the controller. You must not define the primary/secondary

configuration DHCP server you should disable the DHCP proxy. These WLANs drop all DHCP requests and force clients to use a static IP address. These WLANs do not support management over wireless connections.

Restrictions for Internal DHCP Servers

- The controller internal DHCP server does not support Cisco Aironet 600 Series OfficeExtend Access Point.
- Internal DHCP servers are not supported in Cisco Flex 7500 Series Controllers. As a workaround, you can use External DHCP servers.

Configuring DHCP (GUI)

To configure a primary DHCP server for a management, AP-manager, or dynamic interface, see the Configuring Ports and Interfaces chapter.
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 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to assign an interface. The **WLANs > Edit (General)** page appears.

Step 3 On the **General** tab, unselect the **Status** check box and click Apply to disable the WLAN.

Step 4 Reclick the ID number of the WLAN.

Step 5 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 6 Choose the **Advanced** tab to open the **WLANs > Edit (Advanced)** page.

Step 7 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.

Step 8 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.

Note PMIPv6 supports only DHCP based clients and Static IP address is not supported.

Step 9 Click **Apply**.

Step 10 On the General tab, select the **Status** check box and click **Apply** to reenable the WLAN.

Step 11 Click **Save Configuration**.

Configuring DHCP (CLI)

Step 1 Disable the WLAN by entering this command:
config wlan disable *wlan-id*

Step 2 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 3 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.

Note PMIPv6 supports only DHCP based clients and Static IP address is not supported.

Step 4 Reenable the WLAN by entering this command:
config wlan enable *wlan-id*

Debugging DHCP (CLI)

Use these commands to debug DHCP:

- **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

Information About 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.

Guidelines and Limitations

You can configure up to 16 DHCP scopes.

Configuring DHCP Scopes (GUI)

Step 1 Choose **Controller** > **Internal DHCP Server** > **DHCP Scope** to open the **DHCP Scopes** page. This page lists any DHCP scopes that have already been configured.

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 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.

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 Save the configuration.

Step 16 Choose **DHCP Allocated Leases** to see the remaining lease time for wireless clients. The DHCP Allocated Lease page appears, showing the MAC address, IP address, and remaining lease time for the wireless clients.

Configuring DHCP Scopes (CLI)

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:

```
Scope Name            Enabled           Address Range
Scope 1       No       0.0.0.0 -> 0.0.0.0
Scope 2      No    0.0.0.0 -> 0.0.0.0
```

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

Information About MAC Filtering of 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.

When a client tries to associate to a WLAN for the first time, the client gets authenticated with its MAC address from AAA server. If the authentication is successful, the client gets an IP address from DHCP server, and then the client is connected to the WLAN.

When the client roams or sends association request to the same AP or different AP and is still connected to WLAN, the client is not authenticated again to AAA server.

If the client is not connected to WLAN, then the client has to get authenticated from the AAA server.

Configuring Local MAC Filters

Information About Local MAC Filters

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

Configuring Local MAC Filters (CLI)

- 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.
  - *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.

Note If MAC filtering is configured, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local MAC filtering is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured.

Prerequisites for Configuring Local MAC Filters

You must have AAA enabled on the WLAN to override the interface name.

Information About 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.

Configuring Timeout for Disabled Clients (CLI)

- Configure the timeout for disabled clients by entering the **config wlan exclusionlist** *wlan_id timeout* command. The valid timeout range is 1 to 2147483647 seconds. A value of 0 permanently disables 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:

- 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.

For the client with an IPv6 address, controller supports only one untagged interface for a controller. However, in an ideal scenario of IPv4 address, the controller supports one untagged interface per port.

Configuring the DTIM Period

Information About DTIM Period

In the 802.11 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 (to transmit broadcast and multicast frames after every beacon) or 2 (to transmit after every other beacon). For instance, if the beacon period of the 802.11 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 are suitable for applications, including Voice Over IP (VoIP), that expect frequent broadcast and multicast frames.

However, the DTIM value can be set as high as 255 (to transmit broadcast and multicast frames after every 255th beacon) if all 802.11 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 which results in a longer battery life. For example, if the beacon period is 100 ms and you set the DTIM value to 100, the access point transmits buffered broadcast and multicast frames once every 10 seconds. This rate allows the power-saving clients to sleep longer before they have to wake up and listen for broadcasts and multicasts, which results 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. For example, a configured beacon period of 100 ms results 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 that you set a low DTIM value for 802.11 networks that support such clients.

You can configure the DTIM period for the 802.11 radio networks on specific WLANs. For example, you might want to set different DTIM values for voice and data WLANs.

Guidelines and Limitations

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.

Configuring the DTIM Period (GUI)

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**.

Step 5 Choose the **Advanced** tab to open the 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**.

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**.

Configuring the DTIM Period (CLI)

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

Step 2 Configure the DTIM period for a 802.11 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*

Configuring Peer-to-Peer Blocking

Information About Peer-to-Peer Blocking

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. Peer-to-Peer enables you to 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.

Peer-to-peer blocking is supported for clients that are associated with the local switching WLAN.

Per WLAN, peer-to-peer configuration is pushed by the controller to FlexConnect AP. 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.

Restrictions for 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.
- 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.
- In FlexConnect, solution peer-to-peer blocking configuration cannot be applied only to a particular FlexConnect AP or a subset of APs. It is applied to all FlexConnect APs that broadcast the SSID.
- Unified solution for central switching clients supports peer-to-peer upstream-forward. However, this is not supported in the FlexConnect solution. This is treated as peer-to-peer drop and client packets are dropped.
- Unified solution for central switching clients supports peer-to-peer blocking for clients associated with different APs. However, this solution targets only clients connected to the same AP. FlexConnect ACLs can be used as a workaround for this limitation.

Configuring Peer-to-Peer Blocking (GUI)

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.

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.

  Note To enable peer-to-peer blocking on a WLAN configured for FlexConnect local switching, select **Drop** from the P2P Blocking drop-down list and select the **FlexConnect Local Switching** check box.

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

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

Configuring Peer-to-Peer Blocking (CLI)

Step 1 Configure a WLAN for peer-to-peer blocking by entering this command:
config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

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

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

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
...
...
...
Peer-to-Peer Blocking Action..................... Disabled
Radio Policy..................................... All
Local EAP Authentication..................... Disabled
```

Configuring Layer 2 Security

Configuring Static WEP Keys (CLI)

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).

Configuring Dynamic 802.1X Keys and Authorization (CLI)

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.

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 802.11r BSS Fast Transition

Information About 802.11r Fast Transition

802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). The initial handshake allows the client and APs to do the Pairwise Transient Key (PTK) calculation in advance. These PTK keys are applied to the client and AP after the client does the reassociation request or response exchange with new target AP.

802.11r provides two methods of roaming:

- Over-the-Air
- Over-the-DS (Distribution System)

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring reauthentication at every AP. WLAN configuration contains a new Authenticated Key Management (AKM) type called FT (Fast Transition).

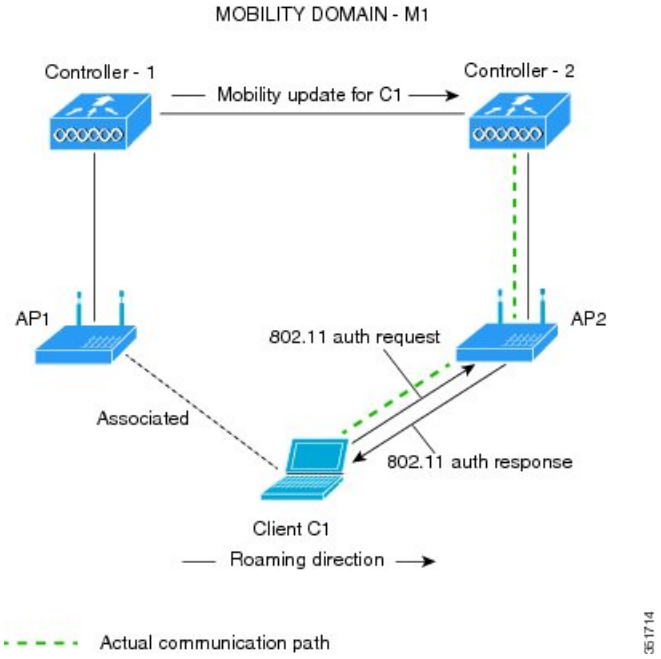
How a Client Roams

For a client to move from its current AP to a target AP using the FT protocols, the message exchanges are performed using one of the following two methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm.
- Over-the-DS—The client communicates with the target AP through the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP and is then sent through the controller.

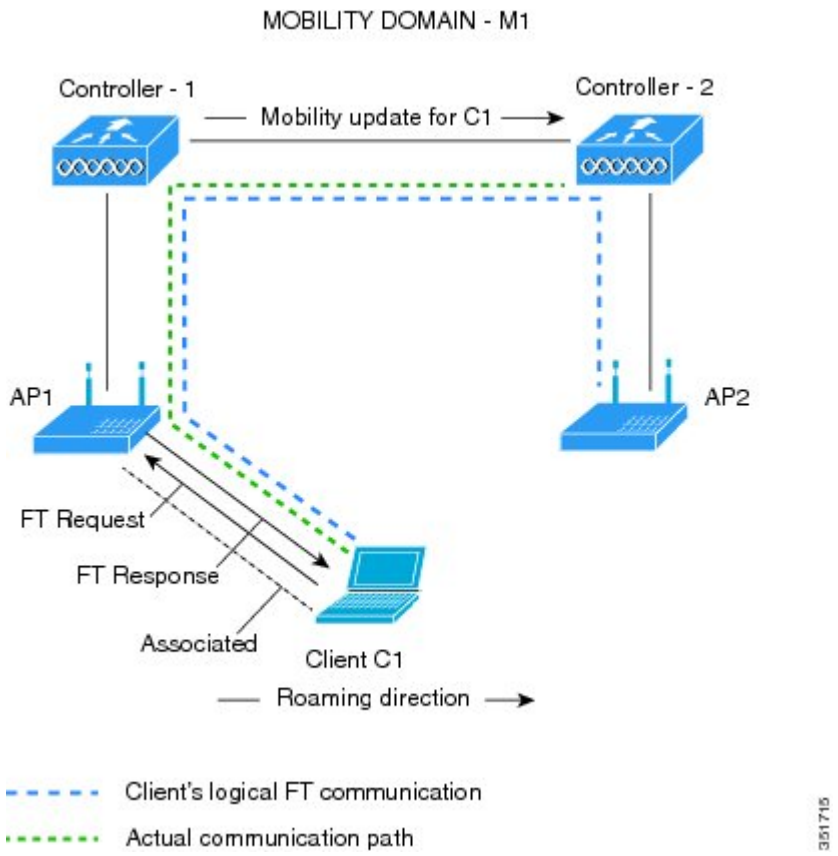
This figure shows the sequence of message exchanges that occur when Over the Air client roaming is configured.

Figure 1: Message Exchanges when Over the Air client roaming is configured



This figure shows the sequence of message exchanges that occur when Over the DS client roaming is configured.

Figure 2: Message Exchanges when Over the DS client roaming is configured



Restrictions for 802.11r Fast Transition

- This feature is not supported on Mesh access points.
- In 8.1 and earlier releases, this feature is not supported on access points in FlexConnect mode. In Release 8.2, this restriction is removed.
- This feature is not supported on Linux-based APs such as Cisco 600 Series OfficeExtend Access Points.
- 802.11r client association is not supported on access points in standalone mode.
- 802.11r fast roaming is not supported on access points in standalone mode.
- 802.11r fast roaming between local authentication and central authentication WLAN is not supported.
- 802.11r fast roaming is not supported if the client uses Over-the-DS preauthentication in standalone mode.
- For APs in FlexConnect mode, 802.11r fast roaming works only if the APs are in the same FlexConnect group.
- EAP LEAP method is not supported. WAN link latency prevents association time to a maximum of 2 seconds.

- The service from standalone AP to client is only supported until the session timer expires.
- TSpec is not supported for 802.11r fast roaming. Therefore, RIC IE handling is not supported.
- If WAN link latency exists, fast roaming is also delayed. Voice or data maximum latency should be verified. The controller handles 802.11r Fast Transition authentication request during roaming for both Over-the-Air and Over-the-DS methods.
- This feature is supported only on open and WPA2 configured WLANs.
- Legacy clients cannot associate with a WLAN that has 802.11r enabled if the driver of the supplicant that is responsible for parsing the Robust Security Network Information Exchange (RSN IE) is old and not aware of the additional AKM suites in the IE. Due to this limitation, clients cannot send association requests to WLANs. These clients, however, can still associate with non-802.11r WLANs. Clients that are 802.11r capable can associate as 802.11i clients on WLANs that have both 802.11i and 802.11r Authentication Key Management Suites enabled.

  The workaround is to enable or upgrade the driver of the legacy clients to work with the new 802.11r AKMs, after which the legacy clients can successfully associate with 802.11r enabled WLANs.

  Another workaround is to have two SSIDs with the same name but with different security settings (FT and non-FT).
- Fast Transition resource request protocol is not supported because clients do not support this protocol. Also, the resource request protocol is an optional protocol.
- To avoid any Denial of Service (DoS) attack, each controller allows a maximum of three Fast Transition handshakes with different APs.
- For APs in FlexConnect mode, 802.11r fast roaming works only if the APs are in the same FlexConnect group.

Configuring 802.11r Fast Transition (GUI)

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

Step 2 Click the WLAN ID to open the WLANs > Edit page.

Step 3 Choose the **Security** > **Layer 2** tab.

Step 4 From the Layer 2 Security drop-down list, choose **WPA+WPA2**.
The Authentication Key Management parameters for Fast Transition appear.

Step 5 Select or unselect the **Fast Transition** check box to enable or disable Fast Transition on the WLAN.

Step 6 Select or unselect the **Over the DS** check box to enable or disable Fast Transition over a distributed system.
This option is available only if you enable Fast Transition.

Step 7 In the Reassociation Timeout box, enter the number of seconds after which the reassociation attempt of a client to an AP should time out.
The valid range is 1 to 100 seconds.

This option is available only if you enable Fast Transition.

Step 8 Under Authentication Key Management, choose between **FT 802.1X** or **FT PSK**. Select or unselect the corresponding check boxes to enable or disable the keys. If you select the **FT PSK** check box, then, from the PSK Format drop-down list, choose **ASCII** or **Hex** and enter the key value.

Step 9 From the WPA gtk-randomize State drop-down list, choose **Enable** or **Disable** to configure the WPA group temporal key (GTK) randomize state.

Step 10 Click **Apply** to save your settings.

Configuring 802.11r Fast Transition (CLI)

Step 1 To enable or disable 802.11r fast transition parameters, use the **config wlan security ft** {**enable** | **disable**} *wlan-id* command.
By default, the fast transition is disabled.

Step 2 To enable or disable 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* command.
By default, the fast transition over a distributed system is disabled.

Step 3 To enable or disable the authentication key management for fast transition using preshared keys (PSK), use the **config wlan security wpa akm ft-psk** {**enable** | **disable**} *wlan-id* command.
By default, the authentication key management using PSK is disabled.

Step 4 To enable or disable the authentication key management for fast transition using 802.1X, use the **config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* command.
By default, the authentication key management using 802.1X is disabled.

Step 5 To enable or disable 802.11r fast transition reassociation timeout, use the **config wlan security ft reassociation-timeout** *timeout-in-seconds wlan-id* command.
The valid range is 1 to 100 seconds. The default value of reassociation timeout is 20 seconds.

Step 6 To enable or disable the authentication key management for fast transition over a distributed system, use the **config wlan security wpa akm ft over-the-ds** {**enable** | **disable**} *wlan-id* command.
By default, the authentication key management for fast transition over a distributed system is enabled.

Step 7 To view the fast transition configuration on a client, use the **show client detailed** *client-mac* command.

Step 8 To view the fast transition configuration on a WLAN, use the **show wlan** *wlan-id* command.

Step 9 To enable or disable debugging of fast transition events, use the **debug ft events** {**enable** | **disable**} command.

Step 10 To enable or disable debugging of key generation for fast transition, use the **debug ft keys** {**enable** | **disable**} command.

Troubleshooting 802.11r BSS Fast Transition

Symptom	Resolution
Non-802.11r legacy clients are no longer connecting.	Check if the WLAN has FT enabled. If so, non-FT WLAN will need to be created.
When configuring WLAN, the FT setup options are not shown.	Check if WPA2 is being used (802.1x / PSK). FT is supported only on WPA2 and OPEN SSIDs.
802.11r clients appear to reauthenticate when they do a Layer 2 roam to a new controller.	Check if the reassociation timeout has been lowered from the default of 20 by navigating to **WLANs** > *WLAN Name* > **Security** > **Layer 2** on the controller GUI.

Configuring MAC Authentication Failover to 802.1X Authentication

You can configure the controller to start 802.1X authentication when MAC authentication with static WEP for the client fails. If the RADIUS server rejects an access request from a client instead of deauthenticating the client, the controller can force the client to undergo an 802.1X authentication. If the client fails the 802.1X authentication too, then the client is deauthenticated.

If MAC authentication is successful and the client requests for an 802.1X authentication, the client has to pass the 802.1X authentication to be allowed to send data traffic. If the client does not choose an 802.1X authentication, the client is declared to be authenticated if the client passes the MAC authentication.

Configuring MAC Authentication Failover to 802.1x Authentication (GUI)

Step 1 Choose **WLANs** > **WLAN ID** to open the WLANs > Edit page.

Step 2 In the **Security** tab, click the **Layer 2** tab.

Step 3 Select the **MAC Filtering** check box.

Step 4 Select the **Mac Auth or Dot1x** check box.

Configuring MAC Authentication Failover to 802.1X Authentication (CLI)

To configure MAC authentication failover to 802.1X authentication, enter this command:
config wlan security 802.1X on-macfilter-failure {**enable** | **disable**} *wlan-id*

Configuring a WLAN for Both Static and Dynamic WEP

Information About 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.

By default, WPA1 uses Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC) for data protection while WPA2 uses the stronger Advanced Encryption Standard encryption algorithm using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP). Both WPA1 and WPA2 use 802.1X for authenticated key management by default. However, these options are also available:

- 802.1X—The standard for wireless LAN security, as defined by IEEE, is called 802.1X for 802.11, or simply 802.1X. An access point that supports 802.1X acts as the interface between a wireless client and an authentication server, such as a RADIUS server, to which the access point communicates over the wired network. If 802.1X is selected, only 802.1X clients are supported.
- 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.

- 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.

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.

Restrictions for Configuring Static and Dynamic WEP

- 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.
- The 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. For more information about CCX, see the Configuring Cisco Client Extensions section.
- In a unified architecture where multiple VLAN clients are supported for a WGB, you also need to configure encryption cipher suite and WEP keys globally, when the WEP encryption is enabled on the WGB. Otherwise, multicast traffic for wired VLAN clients fail.

Configuring WPA1 +WPA2

Configuring WPA1+WPA2 (GUI)

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.

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.

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.

Configuring WPA1+WPA2 (CLI)

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

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

Note You can enable or disable TKIP encryption only using the CLI. Configuring TKIP encryption is not supported in GUI.

When you have VLAN configuration on WGB, you need to configure the encryption cipher mode and keys for a particular VLAN, for example, **encryption vlan 80 mode ciphers tkip**. Then, you need configure the encryption cipher mode globally on the multicast interface by entering the following command: **encryption mode ciphers tkip**.

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 Enable or disable authentication key management suite for fast transition by entering this command:
config wlan security wpa akm ft {**802.1X** | **psk**} {**enable** | **disable**} *wlan_id*

Note You can now choose between the PSK and the fast transition PSK as the AKM suite.

Step 9 Enable or disable randomization of group temporal keys (GTK) between AP and clients by entering this command:
config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

Step 10 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

If you enabled WPA2 with 802.1X authenticated key management, the controller supports both opportunistic PMKID caching and sticky (or non-opportunistic) PMKID caching. In sticky PMKID caching (SKC), the client stores multiple PMKIDs, a different PMKID for every AP it associates with. Opportunistic PMKID caching (OKC) stores only one PMKID per client. By default, the controller supports OKC.

Step 11 Enable the WLAN by entering this command:
config wlan enable wlan_id

Step 12 Save your settings by entering this command:
save config

Configuring Sticky PMKID Caching

Information About Sticky Key Caching

The controller supports sticky key caching (SKC). With sticky key caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client.

In SKC, the client stores each Pairwise Master Key ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

Restrictions for Sticky Key Caching

- The controller supports SKC for up to eight APs per client. If a client roams to more than 8 APs per session, the old APs are removed to store the newly cached entries when the client roams. We recommend that you do not use SKC for large scale deployments.
- SKC works only on WPA2-enabled WLANs.
- SKC does not work across controllers in a mobility group.
- SKC works only on local mode APs.

Configuring Sticky Key Caching (CLI)

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

Step 2 Enable sticky key caching by entering this command:
config wlan security wpa wpa2 cache sticky enable *wlan_id*

By default, SKC is disabled and opportunistic key caching (OKC) is enabled.

Note SKC works only on WPA2 enabled WLANs.

You can check if SKC is enabled by entering this command:

show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 2
Profile Name..................................... new
Network Name (SSID).............................. new
Status........................................... Disabled
MAC Filtering.................................... Disabled
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE)............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
      Auth Key Management
         802.1x.................................. Disabled
         PSK..................................... Enabled
         CCKM.................................... Disabled
         FT(802.11r)............................. Disabled
         FT-PSK(802.11r)......................... Disabled
      SKC Cache Support..... Enabled
```

```
      FT Reassociation Timeout..................... 20
      FT Over-The-Air mode......................... Enabled
      FT Over-The-Ds mode.......................... Enabled
CCKM tsf Tolerance................................. 1000
   Wi-Fi Direct policy configured................. Disabled
   EAP-Passthrough................................ Disabled
```

Step 3 Enable the WLAN by entering this command:
config wlan enable *wlan_id*

Step 4 Save your settings by entering this command:
save config

Configuring CKIP

Information About 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.

Note CKIP is supported for use only with static WEP. It is not supported for use with dynamic WEP. Therefore, a wireless client that is configured to use CKIP with dynamic WEP is unable to associate to a WLAN that is configured for CKIP. We recommend that you use either dynamic WEP without CKIP (which is less secure) or WPA/WPA2 with TKIP or AES (which are more secure).

Configuring CKIP (GUI)

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.

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.

Configuring CKIP (CLI)

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

Information About Session Timeouts

You can configure a WLAN with a session timeout. The session timeout is the maximum time for a client session to remain active before requiring reauthorization.

Configuring Session Timeouts

Configuring a Session Timeout (GUI)

Configurable session timeout range is:

- 300-86400 for 802.1x.
- 0-65535 for all other security types.

Note If you configure session timeout as 0, it means disabling session-timeout, in case of open system, and 86400 seconds for all other system types.

Note When a 802.1x WLAN session timeout value is modified, the associated clients pmk-cache does not change to reflect the new session time out value.

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. Not selecting the checkbox is equal to setting it to 0, which is the maximum value for a session timeout for each session type.

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

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

Configuring a Session Timeout (CLI)

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 Using VPN Passthrough

Information About 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.

Restrictions for Layer 3 Security Using VPN Passthrough

- Layer 2 Tunnel Protocol (L2TP) and IPsec are not supported on controllers.
- Layer 3 security settings are not supported when you disable the client IP address on a WLAN.
- The VPN Passthrough option is not available on Cisco 5500 Series Controllers. However, you can replicate this functionality on the controller by creating an open WLAN using an ACL.

Configuring VPN Passthrough

Configuring VPN Passthrough (GUI)

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 gateway 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.

Configuring VPN Passthrough (CLI)

Use these commands to configure VPN passthrough:

- **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

Configuring Layer 3 Security Using Web Authentication

Information About 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.

Prerequisites for Configuring Web Authentication on a WLAN

- To initiate HTTP/HTTPS web authentication redirection, use HTTP URL or HTTPS URL.
- If the CPU ACLs are configured to block HTTP / HTTPS traffic, after the successful web login authentication, there could be a failure in the redirection page.
- Before enabling web authentication, make sure that all proxy servers are configured for ports other than port 53.
- 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.
- 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.

Additional Information

For more information on using web authentication, see Managing User Accounts.

Configuring Web Authentication

Configuring Web Authentication (GUI)

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.

Configuring Web Authentication (CLI)

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

Configuring Captive Bypassing

Information About Captive Bypassing

WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (For example, Apple iOS devices) have a mechanism using which they can determine if the device is connected to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used for the device to automatically open a web browser when a direct connection to the internet is not possible. This enables the user to provide his credentials to access the internet. The actual authentication is done in the background every time the device connects to a new SSID.

This HTTP request triggers a web authentication interception in the controller as any other page requests are performed by a wireless client. This interception leads to a web authentication process, which will be completed normally. If the web authentication is being used with any of the controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is aborted, and the device processes the page request, thus breaking the splash page functionality.

For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to http://www.apple.com/library/test/success.html for Apple IOS version 6 and older, and to several possible target URLs for Apple IOS version 7 and later. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an ISE captive portal. The controller prevents this pseudo-browser from popping up.

You can now configure the controller to bypass WISPr detection process, so the web authentication interception is only done when a user requests a web page leading to splash page load in user context, without the WISPr detection being performed in the background.

Configuring Captive Bypassing (CLI)

Use these commands to configure captive bypassing:

- **config network web-auth captive-bypass** {**enable** | **disable**}**—**Enables or disables the controller to support bypass of captive portals at the network level.
- **show network summary—**Displays the status for the WISPr protocol detection feature.

Configuring a Fallback Policy with MAC Filtering and Web Authentication

Information About 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.

Restrictions

Mobility is not supported for SSIDs with security type configured for Webauth on MAC filter failure.

Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI)

Note Before configuring a fallback policy, you must have MAC filtering enabled.

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.

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 **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.

Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI)

Note Before configuring a fallback policy, you must have MAC filtering enabled. To know more about how to enable MAC filtering, see the Information About MAC Filtering of WLANs, on page 14 section.

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*

```
FT Over-The-Ds mode.............................. Enabled
CKIP ........................................... Disabled
   IP Security.................................. Disabled
   IP Security Passthru......................... Disabled
   Web Based Authentication..................... Enabled-On-MACFilter-Failure
        ACL..................................... Unconfigured
        Web Authentication server precedence:
        1....................................... local
        2....................................... radius
        3....................................... ldap
```

Assigning a QoS Profile to a WLAN

Information About QoS Profiles

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 wireless rate limits can be defined on both upstream and downstream traffic. Rate limits can be defined per SSID and/or specified as a maximum rate limit for all clients. These rate limits can be individually configured.

The access point uses this QoS-profile-specific UP in accordance with the values in the following table to derive the IP DSCP value that is visible on the wired LAN.

Table 1: Access Point QoS Translation Values

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

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 equivalent of the MSB (100) which is 4. The 802.11e UP value of DSCP 32 is 4.

Assigning a QoS Profile to a WLAN (GUI)

Before You Begin

If you have not already done so, configure one or more QoS profiles using the instructions in the Configuring QoS Profiles (GUI) section.

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

Step 2 Click the ID number of the WLAN to which you want to assign a QoS profile.

Step 3 When the **WLANs > Edit** page appears, choose the **QoS** tab.

Step 4 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 5 To define the data rates on a per-user basis, do the following:

a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

c) Define the average real-time rate for UDP traffic per user by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 6 To define the data rates on a per-SSID basis, do the following:

a) Define the average data rate TCP traffic per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic in the WLANs.

c) Define the average real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.
d) Define the peak real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic in the WLANs.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Assigning a QoS Profile to a WLAN (CLI)

If you have not already done so, configure one or more QoS profiles using the instructions in the Configuring QoS Profiles (CLI) section.

Step 1 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 2 To override QoS profile rate limit parameters, enter this command:
config wlan override-rate-limit *wlan-id* {**average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 3 Enter the **save config** command.

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:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist.................................... Disabled
Session Timeout.................................. 0
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... 1.100.163.24
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
...
```

Configuring QoS Enhanced BSS

Information About 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.

Restrictions for QoS Enhanced BSS

- The OEAP 600 Series access points do not support CAC.
- QBSS is disabled by default.
- 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.
- We recommend that aggressive load balancing always be turned off either through the controller GUI or CLI in any wireless network that is supporting voice, regardless of vendor. When aggressive load balancing is turned on, voice clients can hear an audible artifact when roaming, if the handset is refused at its first reassociation attempt.

Additional Information

See Configuring Controller Settings for more information on configuration instruction for load-based CAC.

Configuring QBSS (GUI)

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.

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.

Configuring QBSS (CLI)

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:
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:
config wlan 7920-support ap-cac-limit {**enable** | **disable**} *wlan_id*

Step 6 Reenable the WLAN by entering this command:
config wlan enable *wlan_id*

Step 7 Save your changes by entering this command:
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:
show wlan *wlan_id*

Configuring Media Session Snooping and Reporting

Information About Media Session 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 Cisco Prime Infrastructure. You can enable or disable Voice over IP (VoIP) snooping and reporting for each WLAN.

When you enable VoIP Media Session Aware (MSA) snooping, 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 Cisco Prime Infrastructure 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. Cisco Prime Infrastructure displays failed VoIP call information in the Events page.

Restrictions for 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.

Configuring Media Session Snooping (GUI)

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 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 4 Under 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**.

Step 6 Click **Save Configuration**.

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.
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. For example, log 0 in the figure 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.

Configuring Media Session Snooping (CLI)

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:
show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
...
 FlexConnect Local Switching...................... Disabled
```

```
    FlexConnect 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:
show call-control client callInfo *client_MAC_address*

Information similar to the following appears:

```
Uplink IP/port..................................... 192.11.1.71 / 23870
Downlonk 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:
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. This table explains the possible error codes for failed calls.

Table 2: Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.

Error Code	Integer	Description
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotallowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.
406	notAcceptabl	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.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	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.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	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.
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header text box.
480	temporarilyNotAvailable	The callee's end system was contacted successfully, but the callee is currently unavailable.
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header text box with the value zero.

Error Code	Integer	Description
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	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.
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	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.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	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.

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 Key Telephone System-Based CAC

Information About Key Telephone System-Based CAC

Key Telephone System-based CAC is a protocol that is used in NEC MH240 wireless IP telephones. You can configure the controller to support CAC on KTS-based SIP clients, to process bandwidth request message from such clients, to allocate the required bandwidth on the AP radio, and to handle other messages that are part of the protocol.

When a call is initiated, the KTS-based CAC client sends a Bandwidth Request message to which the controller responds with a Bandwidth Confirm message indicating whether the bandwidth is allocated or not. The call is allowed only if the bandwidth is available. If the client roams from one AP to another, the client sends another Bandwidth Request message to the controller.

Bandwidth allocation depends on the median time calculated using the data rate from the Bandwidth Request message and the packetization interval. For KTS-based CAC clients, the G.711 codec with 20 milliseconds as the packetization interval is used to compute the medium time.

The controller releases the bandwidth after it receives the bandwidth release message from the client. When the client roams to another AP, the controller releases the bandwidth on the previous AP and allocates bandwidth on the new AP, in both intracontroller and intercontroller roaming scenarios. The controller releases the bandwidth if the client is dissociated or if there is inactivity for 120 seconds. The controller does not inform the client when the bandwidth is released for the client due to inactivity or dissociation of the client.

Restrictions for Key Telephone System-Based CAC

- The controller ignores the SSID Capability Check Request message from the clients.
- Preferred call is not supported for KTS CAC clients.
- Reason code 17 is not supported in intercontroller roaming scenarios.
- To make the KTS-based CAC feature functional, ensure that you do the following:
  - Enable WMM on the WLAN
  - Enable ACM at the radio level
  - Enable processing of TSPEC inactivity timeout at the radio level

Configuring KTS-based CAC (GUI)

Before You Begin

To enable KTS-based CAC for a WLAN, ensure that you do the following:

- Set the QoS profile for the WLAN to Platinum.
- Set the WLAN in disabled state.

- Set the FlexConnect Local Switching in disabled state for the WLAN (On the WLANs > Edit page, click the **Advanced** tab and uncheck the **FlexConnect Local Switching** check box).

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 KTS-based CAC policy.

Step 3 On the **WLANs > Edit** page, click the **Advanced** tab.

Step 4 Under Voice, check or uncheck the **KTS based CAC Policy** check box to enable or disable KTS-based CAC for the WLAN.

Step 5 Save the configuration.

Configuring KTS-based CAC (CLI)

Before You Begin

To enable KTS-based CAC for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:

  config wlan qos *wlan-id* **platinum**

- Disable the WLAN by entering the following command:

  config wlan disable *wlan-id*

- Disable FlexConnect Local Switching for the WLAN by entering the following command:

  config wlan flexconnect local-switching *wlan-id* **disable**

Step 1 To enable KTS-based CAC for a WLAN, enter the following command:
config wlan kts-cac enable *wlan-id*

Step 2 To enable the functioning of the KTS-based CAC feature, ensure you do the following:

a) Enable WMM on the WLAN by entering the following command:
config wlan wmm allow *wlan-id*

b) Enable ACM at the radio level by entering the following command:
config 802.11a cac voice acm enable

c) Enable the processing of the TSPEC inactivity timeout at the radio level by entering the following command:
config 802.11a cac voice tspec-inactivity-timeout enable

Related Commands

- To see whether the client supports KTS-based CAC, enter the following command:

  show client detail *client-mac-address*

  Information similar to the following appears:

```
Client MAC Address.............................. 00:60:b9:0d:ef:26
Client Username ................................ N/A
AP MAC Address.................................. 58:bc:27:93:79:90

QoS Level....................................... Platinum
802.1P Priority Tag............................. disabled
KTS CAC Capability.............................. Yes
WMM Support..................................... Enabled
Power Save...................................... ON
```

- To troubleshoot issues with KTS-based CAC, enter the following command:

  debug cac kts enable

- To troubleshoot other issues related to CAC, enter the following commands:
  - **debug cac event enable**
  - **debug call-control all enable**

Configuring Reanchoring of Roaming Voice Clients

Information About 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 You can reanchor roaming of voice clients for each WLAN.

Restrictions for Configuring Reanchoring of Roaming Voice Clients

- The ongoing data session might be affected due to disassociation and then reassociation.
- This feature is supported for TSPEC-based calls and non-TSPEC SIP-based calls only when you enable the admission control.
- This feature is not recommended for use on Cisco 792x phones.

Configuring Reanchoring of Roaming Voice Clients (GUI)

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.

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

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

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

Configuring Reanchoring of Roaming Voice Clients (CLI)

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 Seamless IPv6 Mobility

Information About IPv6 Mobility

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 the Internet global address space to accommodate users and applications that require unique global IP addresses. IPv6 incorporates 128-bit source and destination addresses, which provide significantly more addresses than the 32-bit IPv4 addresses.

To support IPv6 clients across controllers, ICMPv6 messages must be dealt with specially to ensure the IPv6 client remains on the same Layer 3 network. The controllers keep track of IPv6 clients by intercepting the ICMPv6 messages to provide seamless mobility and protect the network from network attacks. The ICMPv6 packets are converted from multicast to unicast and delivered individually per client. This process allows more control. Specific clients can receive specific Neighbor Discovery and Router Advertisement packets, which ensures correct IPv6 addressing and avoids unnecessary multicast traffic.

The configuration for IPv6 mobility is the same as IPv4 mobility and requires no separate software on the client side to achieve seamless roaming. The controllers must be part of the same mobility group. Both IPv4 and IPv6 client mobility are enabled by default.

Prerequisites for Configuring IPv6 Mobility

- Up to eight client addresses can be tracked per client.
- To allow stateful DHCPv6 IP addressing to operate properly, you must have a switch or router that supports the DHCP for IPv6 feature that 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.

To support the seamless IPv6 Mobility, you might need to configure the following:

- Configuring RA Guard for IPv6 Clients
- Configuring RA Throttling for IPv6 Clients
- Configuring IPv6 Neighbor Discovery Caching

Configuring RA Gaurd for IPv6 Clients

Information About RA Guard

IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 Router Advertisement (RA) packets. The RA Guard feature is similar to the RA guard feature of wired networks. RA Guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from wireless clients. If this feature is not configured, malicious IPv6 clients could announce themselves as the router for the network, which would take higher precedence over legitimate IPv6 routers.

RA Guard occurs at the controller. You can configure the controller to drop RA messages at the access point or at the controller. By default, RA Guard is configured at the access point and also enabled in the controller.

All IPv6 RA messages are dropped, which protects other wireless clients and upstream wired network from malicious IPv6 clients.

Note RA guard is also supported in flexconnect local switching mode.

Configuring RA Guard (GUI)

Step 1 Choose **Controller > IPv6 > RA Guard** to open the IPv6 RA Guard page. By default the IPv6 RA Guard on AP is enabled.

Step 2 From the drop-down list, choose **Disable** to disable RA Guard. The controller also displays the clients that have been identified as sending RA packets.

Step 3 Click **Apply** to commit your changes.

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

Configuring RA Guard (CLI)

Use this command to configure RA Guard:

config ipv6 ra-guard ap {**enable** | **disable**}

Configuring RA Throttling for IPv6 Clients

Information about RA Throttling

RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, then an RA is sent back to the client. This is allowed through the controller and unicasted to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

Configuring RA Throttling (GUI)

Step 1 Choose **Controller > IPv6 > RA Throttle Policy** page. By default the IPv6 RA Throttle Policy is disabled. Unselect the check box to disable RA throttle policy.

Step 2 Configure the following parameters:

- **Throttle period—**The period of time for throttling. RA throttling takes place only after the Max Through limit is reached for the VLAN or the Allow At-Most value is reached for a particular router. The range is from 10 seconds to 86400 seconds. The default is 600 seconds.

- **Max Through—**The maximum number of RA packets on a VLAN that can be sent before throttling takes place. The No Limit option allows an unlimited number of RA packets through with no throttling. The range is from 0 to 256 RA packets. The default is 10 RA packets.
- **Interval Option—**This option allows the controller to act differently based on the RFC 3775 value set in IPv6 RA packets.
  - **Passthrough—** Allows any RA messages with the RFC 3775 interval option to go through without throttling.
  - **Ignore—**Causes the RA throttle to treat packets with the interval option as a regular RA and subject to throttling if in effect.
  - **Throttle—**Causes the RA packets with the interval option to always be subject to rate limiting.
- **Allow At-least—**The minimum number of RA packets per router that can be sent as multicast before throttling takes place. The range is from 0 to 32 RA packets.
- **Allow At-most—**The maximum number of RA packets per router that can be sent as multicast before throttling takes place. The No Limit option allows an unlimited number of RA packets through the router. The range is from 0 to 256 RA packets.

Note When RA throttling occurs, only the first IPv6 capable router is allowed through. For networks that have multiple IPv6 prefixes being served by different routers, you should disable RA throttling.

Step 3 Click **Apply** to commit your changes.

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

Configuring the RA Throttle Policy (CLI)

Use this command to configure the RA throttle policy:

config ipv6 neigbhor-binding ra-throttle {**allow at-least** *at-least-value* | **enable** | **disable** | **interval-option** { **ignore** | **passthrough** | **throttle**} | **max-through** {**max-through-value** | **no-limit**}}

Configuring IPv6 Neighbor Discovery Caching

Information About IPv6 Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.

At any given time, only eight IPv6 addresses are supported per client. When the ninth IPv6 address is encountered, the controller removes the oldest stale entry and accommodates the latest one.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery packets that do not comply are dropped. The neighbor binding table in the controller track each IPv6 address and its associated MAC address. Clients are expired from the table according to Neighbor Binding timers.

Configuring Neighbor Binding (GUI)

Step 1 Choose **Controller > IPv6 > Neighbor Binding** page.

Step 2 Configure the following:

- Down–Lifetime—Specifies how long IPv6 cache entries are kept if the interface goes down. The range is from 0 to 86400 seconds.
- Reachable–Lifetime—Specifies how long IPv6 addresses are active. The range is from 0 to 86400 seconds.
- Stale–Lifetime—Specifies how long to keep IPv6 addresses in the cache. The range is from 0 to 86400 seconds.

Step 3 Enable or disable the Unknown Address Multicast NS Forwarding.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Configuring Neighbor Binding (CLI)

- Configure the neighbor binding parameters by entering this command:
  config ipv6 neighbor-binding timers {**down-lifetime** | **reachable-lifetime** | **stale-lifetime**} {**enable** | **disable**}
- Configure the Unknown Address Multicast NS Forwarding by entering this command:
  config ipv6 ns-mcast-fwd {**enable** | **disable**}
- See the status of neighbor binding data that are configured on the controller by entering this command:
  show ipv6 neighbor-binding summary

Configuring Cisco Client Extensions

Information About Cisco Client Extensions

The 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 that are related to increased security, enhanced performance, fast roaming, and power management.

Prerequisites for Configuring Cisco Client Extensions

- The software supports 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 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.

Configuring CCX Aironet IEs (GUI)

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.

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.

Viewing a Client's CCX Version (GUI)

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.

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.
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.

Configuring CCX Aironet IEs (CLI)

Use this command to configure CCX Aironet IEs:

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

The default value is enabled.

Viewing a Client's CCX Version (CLI)

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

show client detail *client_mac*

Configuring Remote LANs

Information About Remote LANs

This section describes how to configure remote LANs.

Restrictions for Configuring Remote LANs

- 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.
- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.

Configuring Remote LANs

Configuring a Remote LAN (GUI)

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.

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.

Configuring a Remote LAN (CLI)

- 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*

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*

Configuring AP Groups

Information About 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 that are 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.

AP Groups Supported on Controller Platforms

This table lists the AP groups supported on various controller platforms:

Controller Platform	AP Groups Supported
Cisco 2500 Series Wireless Controller	50
Cisco 5500 Series Wireless Controller	500
Cisco Virtual Wireless Controller	200
Cisco 7500 Series Wireless Controller	6000
Cisco 8500 Series Wireless Controller	6000
Cisco Wireless Services Module 2	1000

Configuring Access Point Groups

Step 1 Configure the appropriate dynamic interfaces and map them to the desired VLANs.
For example, to implement the network described in the Information About Access Point Groups section, create dynamic interfaces for VLANs 61, 62, and 63 on the controller. See the Configuring Dynamic Interfaces section for information about how to configure dynamic interfaces.

Step 2 Create the access point groups. See the Creating Access Point Groups section.

Step 3 Create a RF profile. See the Creating an RF Profile section.

Step 4 Assign access points to the appropriate access point groups. See the Creating Access Point Groups section.

Step 5 Apply the RF profile on the AP groups. See the Applying RF Profile to AP Groups section.

Creating Access Point Groups (GUI)

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page.
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 The controller creates a default 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 In the **NAS-ID** text box, enter the network access server identifier for the AP group.

Step 6 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 7 Click the name of the group to edit this new group. The **AP Groups > Edit (General)** page appears.

Step 8 Change the description of this access point group by entering the new text in the AP Group Description text box and click **Apply**.

Step 9 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 10 Click **Add New** to assign a WLAN to this access point group. The Add New section appears at the top of the page.

Step 11 From the WLAN SSID drop-down list, choose the SSID of the WLAN.

Step 12 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 13 Select the **SNMP 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.

Step 14 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**.

Step 15 Repeat *Step 10* through *Step 14* to add any additional WLANs to this access point group.

Step 16 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".

Step 17 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, after it is reloaded, appears in the list of access points currently in this access point group. The AP has to be reloaded if the AP has to be moved from one group to another.

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**.

Step 18 Click **Save Configuration**.

Creating Access Point Groups (CLI)

Step 1 Create an access point group by entering this command:
config wlan apgroup add *group_name*

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 wlan-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

Viewing Access Point Groups (CLI)

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

- 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*

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

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

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

  debug group {**enable** | **disable**}

Configuring RF Profiles

Information About RF Profiles

RF Profiles allows you to tune groups of APs that share a common coverage zone together and selectively change how RRM will operates the APs within that coverage zone.

For example, a university might deploy a high density of APs in an area where a high number of users will congregate or meet. This situation requires that you manipulate both data rates and power to address the cell density while managing the co-channel interference. In adjacent areas, normal coverage is provided and such manipulation would result in a loss of coverage.

Using RF profiles and AP groups allows you to optimize the RF settings for AP groups that operate in different environments or coverage zones. RF profiles are created for the 802.11 radios. RF profiles are applied to all APs that belong to an AP group, where all APs in that group will have the same profile settings.

The RF profile gives you the control over the data rates and power (TPC) values.

Note The application of an RF profile does not change the AP's status in RRM. It is still in global configuration mode controlled by RRM.

To address high-density complex RF topologies, the following configurations are available:

- High Density Configurations—The following configurations are available to fine tune RF environments in a dense wireless network:
  - Client limit per WLAN or radio—Maximum number of clients that can communicate with the AP in a high-density environment.
  - Client trap threshold—Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller and Cisco Prime Infrastructure.
- Stadium Vision Configurations—You can configure the following parameter:
  - Multicast data rates—Configurable data rate for multicast traffic based on the RF condition of an AP.
- Out-of-Box AP Configurations—To create an Out-of-Box AP group that consists of newly installed access points that belong to the default AP group. When you enable this feature:
  - Newly installed access points (assigned to the 'default-group' AP group by default) are automatically assigned to the Out-of-Box AP group upon associating with the controller, and their radios are administratively disabled. This eliminates any RF instability caused by the new access points.
  - When Out-of-Box is enabled, default-group APs currently associated with the controller remain in the default group until they reassociate with the controller.
  - All default-group APs that subsequently associate with the controller (existing APs on the same controller that have dropped and reassociated, or APs from another controller) are placed in the Out-of-Box AP group.

    Note When removing APs from the Out-of-Box AP group for production use, we recommend that you assign the APs to a custom AP group to prevent inadvertently having them revert to the Out-of-Box AP group.

  - Special RF profiles are created per 802.11 band. These RF profiles have default settings for all the existing RF parameters and additional new configurations.

Note When you disable this feature after you enable it, only subscription of new APs to the Out of Box AP group stops. All APs that are subscribed to the Out of Box AP Group remain in this AP group. The network administrators can move such APs to the default group or a custom AP group upon network convergence.

- Band Select Configurations— Band Select addresses client distribution between the 2.4-GHz and 5-GHz bands by first understanding the client capabilities to verify whether a client can associate on both 2.4-GHz and 5-GHz spectrum. Enabling band select on a WLAN forces the AP to do probe suppression on the 2.4-GHz band that ultimately moves dual band clients to 5-GHz spectrum. You can configure the following band select parameters per AP Group:
  - Probe response—Probe responses to clients that you can enable or disable.
  - Probe Cycle Count—Probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.

- Cycle Threshold—Time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
- Suppression Expire—Expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
- Dual Band Expire—Expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
- Client RSSI—Minimum RSSI for a client to respond to a probe.

- Load Balancing Configurations—Load balancing maintains fair distribution of clients across APs. You can configure the following parameters:
  - Window—Load balancing sets client association limits by enforcing a client window size. For example, if the window size is defined as 3, assuming fair client distribution across the floor area, then an AP should have no more than 3 clients associated with it than the group average.
  - Denial—The denial count sets the maximum number of association denials during load balancing.

- Coverage Hole Mitigation Configurations—You can configure the following parameters:
  - Data RSSI—Minimum receive signal strength indication (RSSI) value for data packets received by the access point. The value that you enter is used to identify coverage holes (or areas of poor coverage) within your network.
  - Voice RSSI—Minimum receive signal strength indication (RSSI) value for voice packets received by the access point.
  - Coverage Exception—Minimum number of clients on an access point with an RSSI value at or below the data or voice RSSI threshold to trigger a coverage hole exception.
  - Coverage Level—Percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point. If an access point has more number of such clients than the configured coverage level it triggers a coverage hole event.

Prerequisites for Configuring RF Profiles

Once you create an AP group and apply RF profiles or modify an existing AP group, the new settings are in effect and the following rules become effective:

- The same RF profile must be applied and present on every controller of the AP group or the action will fail for that controller.
- You can assign the same RF profile to more than one AP group.

Configuring an RF Profile (GUI)

Step 1 Choose **Wireless** > **RF Profiles** to open the RF profiles page.

Step 2 To configure the out-of-box status for all RF profiles, select or unselect the **Enable Out Of Box** check box.

Step 3 Click **New**.

Step 4 Enter the RF Profile Name and choose the radio band.

Step 5 Click **Apply** to configure the customizations of power and data rate parameters.

Step 6 In the **General** tab, enter the description for the RF profile in the Description text box.

Step 7 In the **802.11** tab, configure the data rates to be applied to the APs of this profile.

Step 8 In the **RRM** tab, do the following:

a) In the TPC area, configure the Maximum and Minimum Power Level Assignment, that is the maximum and minimum power that the APs in this RF profile are allowed to use.

b) In the TPC area, configure a custom TPC power threshold for either Version1 or Version 2 of TPC.

Note Only one version of TPC can be operable for RRM on a given controller Version 1 and Version 2 are not interoperable within the same RF profile. If you select a threshold value for TPCv2 and it is not in the chosen TPC algorithm for the RF profile, this value will be ignored.

c) In the Coverage Hole Detection area, configure the voice and data RSSI.

d) In the Coverage Exception text box, enter the number for clients.

e) In the Coverage Level text box, enter the percentage.

Step 9 In the **High Density** tab, do the following:

a) In the High Density Parameters area, enter the maximum number of clients to be allowed per AP radio and the client trap threshold value.

b) In the Multicast Parameters area, choose the data rates from the Multicast Data Rates drop-down list.

Step 10 In the **Client Distribution** tab, do the following:

a) In the Load Balancing area, enter the client window size and the denial count.
The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing window + client associations on AP with the lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

The denial count sets the maximum number of association denials during load balancing.

b) In the Band Select area, select or unselect the **Probe Response** check box.

Note The Band Select configurations are available only for the 802.11b/g RF profiles.

c) In the Cycle Count text box, enter a value that sets the number of suppression cycles for a new client. The default count is 2.

d) In the Cycle Threshold text box, enter a time period in milliseconds that determines the time threshold during which new probe requests from a client from a new scanning cycle. The default cycle threshold is 200 milliseconds.

e) In the Suppression Expire text box, enter a time period after which the 802.11 b/g clients become new and are subject to probe response suppression.
f) In the Dual Band Expire text box, enter a time period after which the dual band clients become new and are subject to probe response suppression.
g) In the Client RSSI text box, enter the minimum RSSI for a client to respond to a probe.

Step 11 Click **Apply** to commit your changes.

Step 12 Click **Save Configuration** to save your changes.

Configuring an RF Profile (CLI)

Step 1 To configure the out-of-box status for all RF profiles, enter this command:
config rf-profile out-of-box {**enable** | **disable**}

Step 2 To create or delete an RF profile, enter this command:
config rf-profile {**create** {**802.11a** | **802.11b**} | **delete**} *profile-name*

Step 3 To specify a description for the RF profile, enter this command:
config rf-profile description *text profile-name*

Step 4 To configure the data rates to be applied to the APs of this profile, enter this command:
config rf-profile data-rates {**802.11a** | **802.11b**} {**disabled** | **mandatory** | **supported**} *rate profile-name*

Step 5 To configure the maximum and minimum power level assignment, that is the maximum and minimum power that the APs in this RF profile are allowed to use, enter this command:
config rf-profile {**tx-power-max** | **tx-power-min**} *power-value profile-name*

Step 6 To configure a custom TPC power threshold for either Version1 or Version 2 of TPC, enter this command:
config rf-profile {**tx-power-control-thresh-v1** | **tx-power-control-thresh-v2**} *power-threshold profile-name*

Step 7 To configure the coverage hole detection parameters:

a) To configure the coverage data, enter this command:
config rf-profile coverage data *value-in-dBm profile-name*

b) To configure the minimum client coverage exception level, enter this command:
config rf-profile coverage exception *clients profile-name*

c) To configure the coverage exception level percentage, enter this command:
config rf-profile coverage level *percentage-value profile-name*

d) To configure the coverage of voice, enter this command:
config rf-profile coverage voice *value-in-dBm profile-name*

Step 8 To configure the maximum number of clients to be allowed per AP radio, enter this command:
config rf-profile max-clients *num-of-clients profile-name*

Step 9 To configure the client trap threshold value, enter this command:
config rf-profile client-trap-threshold *threshold-value profile-name*

Step 10 To configure multicast, enter this command:
config rf-profile multicast data-rate *rate profile-name*

Step 11 To configure load balancing, enter this command:
config rf-profile load-balancing {**window** *num-of-clients* | **denial** *value*} *profile-name*

Step 12 To configure band select:

a) To configure the band select cycle count, enter this command:
config rf-profile band-select cycle-count *max-num-of-cycles profile-name*

b) To configure the cycle threshold, enter this command:
config rf-profile band-select cycle-threshold *time-in-milliseconds profile-name*

c) To configure the expiry of the band select, enter this command:
config rf-profile band-select expire {**dual-band** | **suppression**} *time-in-seconds profile-name*

d) To configure the probe response, enter this command:
config rf-profile band-select probe-response {**enable** | **disable**} *profile-name*

e) To configure the minimum RSSI for a client to respond to a probe, enter this command:
config rf-profile band-select client-rssi *value-in-dBm profile-name*

Applying an RF Profile to AP Groups (GUI)

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page.

Step 2 Click the AP Group Name to open the AP Group > Edit page.

Step 3 Click the **RF Profile** tab to configure the RF profile details. You can choose an RF profile for each band (802.11a/802.11b) or you can choose just one or none to apply to this group.

Note Until you choose the APs and add them to the new group, no configurations are applied. You can save the new configuration as is, but no profiles are applied. Once you choose the APs to move the AP group, the process of moving the APs into the new group reboots the APs and the configurations for the RF profiles are applied to the APs in that AP group.

Step 4 Click the **APs** tab and choose the APs to add to the AP group.

Step 5 Click **Add APs** to add the selected APs to the AP group. A warning message displays that the AP group will reboot the APs will rejoin the controller.

Note APs cannot belong to two AP groups at once.

Step 6 Click **Apply**. The APs are added to the AP Group.

Applying RF Profiles to AP Groups (CLI)

What to Do Next

Use this command to apply RF profiles to AP groups:

- **config wlan apgroup profile-mapping** {**add** | **delete**} *ap-group-name rf-profile-name*

Configuring Web Redirect with 802.1X Authentication

Information About 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.

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 and the corresponding ACL to allow access to this server in "url-redirect-acl". 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.

Suppose there are backend applications running on the wireless clients and they use HTTP or HTTPS port for their communication. If the applications start communicating before the actual web page is opened, the redirect functionality does not work with web passthrough.

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.

Configuring the RADIUS Server (GUI)

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)**.

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

Configuring Web Redirect

Configuring Web Redirect (GUI)

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.

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.

Configuring Web Redirect (CLI)

Step 1 Enable or disable conditional web redirect by entering this command:
config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Step 2 Enable or disable splash page web redirect by entering this command:
config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Step 3 Save your settings by entering this command:
save config

Step 4 See the status of the web redirect features for a particular WLAN by entering this command:
show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
...
Web Based Authentication........................ Disabled
```

```
Web-Passthrough.............................. Disabled
Conditional Web Redirect..................... Disabled
Splash-Page Web Redirect..................... Enabled
...
```

Disabling Accounting Servers per WLAN (GUI)

Note Disabling accounting servers disables all accounting operations and prevents the controller from falling back to the default RADIUS server for the WLAN.

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.

Step 4 Unselect the **Enabled** check box for the Accounting Servers.

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

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

Disabling Coverage Hole Detection per WLAN

Note Coverage hole detection is enabled globally on the controller.

Note 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.

Disabling Coverage Hole Detection on a WLAN (GUI)

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.

Step 4 Unselect the **Coverage Hole Detection Enabled** check box.

Note OEAP 600 Series Access Points do not support coverage hole detection.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Disabling Coverage Hole Detection on a WLAN (CLI)

Step 1 Disable coverage hole detection on a 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

Information About NAC Out-of-Band Integration

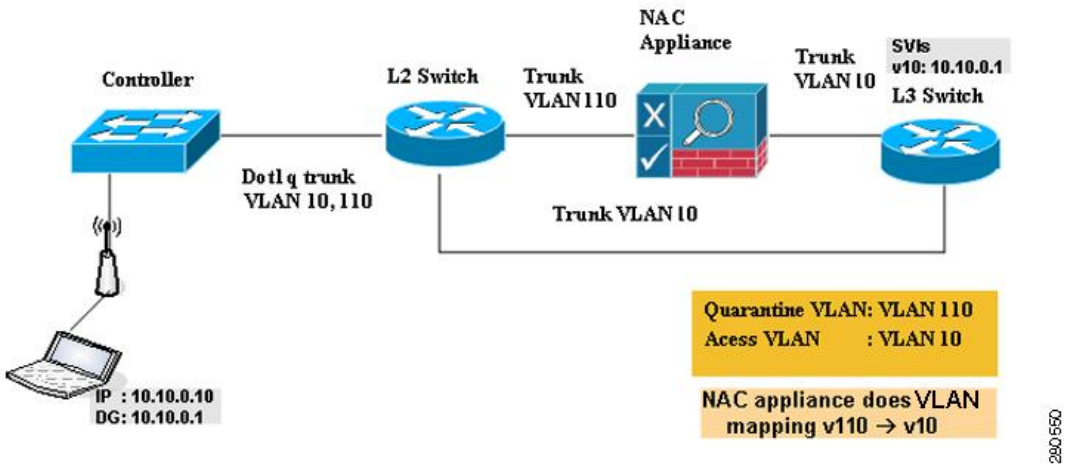
The Cisco NAC Appliance, also known as Cisco Clean Access (CCA), is a network admission control (NAC) product that enables network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. NAC identifies 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).

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 remedial action. After cleaning is completed, the NAC appliance updates the controller to change the client state from Quarantine to Access.

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.

Figure 3: Example of NAC Out-of-Band Integration



Guidelines and Limitations

Configuring NAC Out-of-Band Integration

Configuring NAC Out-of-Band Integration (GUI)

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.
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.
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.
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.
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.

Configuring NAC Out-of-Band Integration (CLI)

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.

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 Clients

Information About Passive Clients

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.

Note For FlexConnect APs with locally switched WLANs, passive client feature enables the broadcast of ARP requests and the APs respond on behalf of the client.

Restrictions for Passive Clients

- The interface associated to the WLAN must have a VLAN tagging.
- GARP forwarding must to be enabled using the **show advanced hotspot** command.

Note Client ARP forwarding will not work if any one of the two scenarios, mentioned above, is not configured.

- The passive client feature is not supported with the AP groups and FlexConnect centrally switched WLANs.

Configuring Passive Clients (GUI)

Before You Begin

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

Step 1 Choose **Controller** > **General** to open the 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 From the **AP Multicast Mode** drop-down list, choose**Multicast**. 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**.

Step 6 Enable global multicast mode as follows:

a) Choose **Controller** > **Multicast**.

b) Select the **Enable Global Multicast Mode** check box.

Enabling the Multicast-Multicast Mode (GUI)

Before You Begin

To configure passive clients, you must enable multicast-multicast or multicast-unicast mode.

Step 1 Choose **Controller** > **General** to open the 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 From the **AP Multicast Mode** drop-down list, choose **Multicast**. The **Multicast Group Address** text box is displayed.

Note It is not possible to configure the AP multicast mode for Cisco Flex 7500 Series controllers because only unicast is supported.

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

Step 5 Click **Apply**.

Step 6 Enable global multicast mode as follows:

a) Choose **Controller** > **Multicast**.

b) Select the **Enable Global Multicast Mode** check box.

Enabling the Global Multicast Mode on Controllers (GUI)

Step 1 Choose **Controller** > **Multicast** to open the Multicast page.

Note 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.

Note It is not possible to configure Global Multicast Mode for Cisco Flex 7500 Series Controllers.

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 (GUI)

Step 1 Choose **WLANs** > **WLANs** > **WLAN ID** to open the WLANs > Edit page. By default, the General tab is displayed.

Step 2 Choose the **Advanced** tab.

Step 3 Select the **Passive Client** check box to enable the passive client feature.

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

Configuring Passive Clients (CLI)

Step 1 Enable multicasting on the controller by entering this command:
config network multicast global enable

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 *2*

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*

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

Note Cisco WLC detects duplicate IP addresses based on the ARP table, and not based on the VLAN information. If two clients in different VLANs are using the same IP address, Cisco WLC reports IP conflict and sends GARP. This is not limited to two wired clients, but also for a wired client and a wireless client.

Configuring Client Profiling

Information About Client Profiling

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form. Local Client profiling (DHCP and HTTP) is enabled at WLAN level. Clients on the WLANS will be profiled as soon as profling is enabled.

Wireless LAN Controller has been enhanced with some of these following capabilities:

- WLC does profiling of devices based on protocols like HTTP, DHCP, etc. to identify the end devices on the network.
- You can configure device-based policies and enforce per user or per device end points, and policies applicable per device.
- WLC displays statistics based on per user or per device end points, and policies applicable per device.

Profiling can be based on:

- Role, defining the user type or the user group to which the user belongs.
- Device type, such as Windows machine, Smart Phone, iPad, iPhone, Android, etc.
- Username/ password pair.
- Location, based on the AP group to which the endpoint is connected
- Time of the day, based on what time of the day the endpoint is allowed on the network.
- EAP type, to check what EAP method the client uses to get connected.

Policing is decided based on a profile which are:

- VLAN
- QoS Level
- ACL
- Session timeout value

Restrictions for Configuring Client Profiling

- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
  - Wired clients behind the WGB will not be profiled and policy action will not be done.
- With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.
- While the controller parses the DHCP profiling information every time the client sends a request, the profiling information is sent to ISE only once.
- Custom profiles cannot be created for this release.
- This release contains 88 pre-existing policies where CLI is check only except if you create a policy.
- When local profiling is enabled radius profiling is not allowed on a particular WLAN.
- Only the first policy rule that matches is applied.

- Only 16 policies per WLAN can be configured and globally 16 policies can be allowed.
- Policy action is done only after L2/L3 authentication is complete or when the device sends http traffic and gets the device profiled. Profiling and policing actions will happen more than once per client.
- If AAA override is enabled and if you get any AAA attributes from the AAA server other than role type, configured policy does not apply since the AAA override attributes have a higher precedence.

Configuring Client Profiling

Configuring Client Profiling (GUI)

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

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

Step 3 Click the **Advanced** tab.

Step 4 In the Client Profiling area, do the following:

a) To profile clients based on HTTP, select the **HTTP Profiling** check box.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Client Profiling (CLI)

- Enable or disable client profiling in RADIUS mode for a WLAN based on HTTP, DHCP, or both by entering this command:

  config wlan profiling radius {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

  Note Use the **all** parameter to configure client profiling based on both DHCP and HTTP.

- To see the status of client profiling on a WLAN, enter the following command:

  show wlan *wlan-id*

- To enable or disable debugging of client profiling, enter the following command:

  debug profiling {**enable** | **disable**}

Configuring Per-WLAN RADIUS Source Support

Information About Per-WLAN RADIUS Source Support

The controller sources RADIUS traffic from the IP address of its management interface unless the configured RADIUS server exists on a VLAN accessible via one of the controller Dynamic interfaces. If a RADIUS server is reachable via a controller Dynamic interface, RADIUS requests to this specific RADIUS server will be sourced from the controller via the corresponding Dynamic interface.

By default, RADIUS packets sourced from the controller will set the NAS-IP-Address attribute to that of the management interface's IP Address, regardless of the packet's source IP Address (Management or Dynamic, depending on topology).

When you enable per-WLAN RADIUS source support (Radius Server Overwrite interface) the NAS-IP-Address attribute is overwritten by the controller to reflect the sourced interface. Also, RADIUS attributes are modified accordingly to match the identity. This feature virtualizes the controller on the per-WLAN RADIUS traffic, where each WLAN can have a separate layer 3 identity. This feature is useful in deployments that integrate with ACS Network Access Restrictions and Network Access Profiles.

To filter WLANs, use the callStationID that is 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.

You can combine per-WLAN RADIUS source support with the normal RADIUS traffic source and some WLANs that use the management interface and others using the per-WLAN dynamic interface as the address source.

Restrictions for Per-WLAN RADIUS Source Support

- 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.

Configuring Per-WLAN RADIUS Source Support (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 Enable either an AP group's interface or a WLAN's interface for RADIUS packet routing by entering these commands:

- AP group's interface—**config wlan radius_server overwrite-interface apgroup** *wlan-id*
- WLAN's interface—**config wlan radius_server overwrite-interface wlan** *wlan-id*

Note Valid WLAN ID range is between 1 and 16.

Step 4 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 (CLI)

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 *1*

Information similar to the following is displayed:

```
WLAN Identifier.................................. 4
Profile Name..................................... example
Network Name (SSID).............................. example
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
```

Configuring Remote LANs

Information About Remote LANs

This section describes how to configure remote LANs.

Restrictions for Configuring Remote LANs

- 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.

- It is not possible to configure 802.1X on remote LANs through the controller GUI; configuration only through CLI is supported.

Configuring Remote LANs

Configuring a Remote LAN (GUI)

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.

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.

Configuring a Remote LAN (CLI)

- 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*

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*