Configuring Mobile Concierge

Information About Mobile Concierge

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

Configuring Mobile Concierge (802.11u)

Configuring Mobile Concierge (802.11u) (GUI)

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

Step 2 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the 802.11u parameters and select 802.11u. The 802.11u page appears.

Step 3 Select the **802.11u Status** check box to enable 802.11u on the WLAN.

Step 4 In the 802.11u General Parameters area, do the following:

a) Select the **Internet Access** check box to enable this WLAN to provide Internet services.

b) From the Network Type drop-down list, choose the network type that best describes the 802.11u you want to configure on this WLAN.

c) From the Network Auth Type drop-down list, choose the authentication type that you want to configure for the 802.11u parameters on this network.

d) In the HESSID box, enter the homogenous extended service set identifier (HESSID) value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

e) If the IP address is in the IPv4 format, then from the IPv4 Type drop-down list, choose the IPv4 address type.

f) From the IPv6 Type drop-down list, choose whether you want to make the IPv6 address type available or not.

Step 5 In the OUI List area, do the following:

a) In the OUI text box, enter the Organizationally Unique Identifier, which can be a hexadecimal number represented in 3 or 5 bytes (6 or 10 characters). For example, AABBDF.

b) Select the **Is Beacon** check box to enable the OUI beacon responses.

Note You can have a maximum of 3 OUIs with this field enabled.

c) From the OUI Index drop-down list, choose a value from 1 to 32. The default is 1.

d) Click **Add** to add the OUI entry to the WLAN.
To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 6 In the Domain List area, do the following:

a) In the Domain Name box, enter the domain name that is operating in the WLAN.

b) From the Domain Index drop-down list, choose an index for the domain name from 1 to 32. The default is 1.

c) Click **Add** to add the domain entry to the WLAN.
To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 7 In the Realm List area, do the following:

a) In the Realm text box, enter the realm name that you can assign to the WLAN.

b) From the Realm Index drop-down list, choose an index for the realm from 1 to 32. The default is 1.

c) Click **Add** to add the domain entry to this WLAN.
To remove this entry, hover your mouse pointer over the blue drop-down image and choose **Remove**.

Step 8 In the Cellular Network Information List area, do the following:

a) In the Country Code text box, enter the 3-character mobile country code.

b) From the CellularIndex drop-down list, choose a value between 1 and 32. The default is 1.

c) In the Network Code text box, enter the character network code. The network code can be 2 or 3 characters.
d) Click **Add** to add the cellular network information to the WLAN.
To remove this entry, hover your mouse pointer over the blue drop-down image and select **Remove**.

Step 9 Click **Apply**.

Configuring Mobile Concierge (802.11u) (CLI)

- To enable or disable 802.11u on a WLAN, enter this command:
config wlan hotspot dot11u {**enable** | **disable**} *wlan-id*
- To add or delete information about a third generation partnership project's cellular network, enter this command:
config wlan hotspot dot11u 3gpp-info {**add** *index mobile-country-code network-code wlan-id* | **delete** *index wlan-id*}
- To configure the domain name for the entity operating in the 802.11u network, enter this command:
config wlan hotspot dot11u domain {{{**add** | **modify**} *wlan-id domain-index domain-name*} | {**delete** *wlan-id domain-index*}}
- To configure a homogenous extended service set identifier (HESSID) value for a WLAN, enter this command:
config wlan hotspot dot11u hessid *hessid wlan-id*

  The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.
- To configure the IP address availability type for the IPv4 and IPv6 IP addresses on the WLAN, enter this command:
config wlan hotspot dot11u ipaddr-type *ipv4-type ipv6-type wlan-id*
- To configure the network authentication type, enter this command:
config wlan hotspot dot11u auth-type *network-auth wlan-id*
- To configure the Roaming Consortium OI list, enter this command:
config wlan hotspot dot11u roam-oi {{{**add** | **modify**} *wlan-id oi-index oi is-beacon*} | {**delete** *wlan-id oi-index*}}
- To configure the 802.11u network type and internet access, enter this command:
config wlan hotspot dot11u network-type *wlan-id network-type internet-access*
- To configure the realm for the WLAN, enter this command:
config wlan hotspot dot11u nai-realm {{{**add** | **modify**} *realm-name wlan-id realm-index realm-name* | {**delete** *realm-name wlan-id realm-index*}}
- To configure the authentication method for the realm, enter this command:
config wlan hotspot dot11u nai-realm {**add** | **modify**} **auth-method** *wlan-id realm-index eap-index auth-index auth-method auth-parameter*
- To delete the authentication method for the realm, enter this command:
config wlan hotspot dot11u nai-realm delete auth-method *wlan-id realm-index eap-index auth-index*
- To configure the extensible authentication protocol (EAP) method for the realm, enter this command:

config wlan hotpspot dot11u nai-realm {**add** | **modify**} **eap-method** *wlan-id realm-index eap-index eap-method*

- To delete the EAP method for the realm, enter this command:
  config wlan hotspot dot11u nai-realm delete eap-method *wlan-id realm-index eap-index*

Online Sign Up

Online Sign Up (OSU) is a process in which a mobile device is registered with a service provider, enabling users to select a plan to obtain network access. After the sign-up, the device receives the users' credentials to connect to the network. A network architecture for OSU is given below, which consists of a service provider network and a hotspot:

The service provider network consists of an OSU server, an Authentication, Authorization and Accounting (AAA) server, and (access to) a Certification Authority (CA). These devices may be co-located or separate.

The hotspot has its own OSU, which is optional, and a AAA server. The hotspot is configured to allow only HTTPS traffic to OSU servers. An OSU server registers new customers and provides security credentials to their mobile devices. It can also be used to initially provision devices of existing customers. The AAA server of the service provider is used to authenticate subscribers based on the information received from the OSU server.

The OSU process ensures that:

- A user is communicating with the intended service provider network and OSU server.
- The communication is protected between the mobile device and OSU server.
- Poor security practices of one service provider affecting other service providers are reduced.

The Cisco Wireless LAN Controller (WLC) should support the following requirements:

- Hotspot 2.0 Indication Element
- OSU Service Provider List
- Icon Request and Response Access Network Query Protocol (ANQP) Element
- OSU Server-Only Authenticated L2 Encryption Network (OSEN)
- Wireless Network Management (WNM) Notification Subscription Remediation Request
- WNM Notification Deauth Imminent Request
- Basic Service Set (BSS) Transition Management Request Frame - Session URL
- QoS Map Set
- Extended Capability Bit Support:
  - WNM Notification
  - QoS Map Set

Hotspot 2.0 Indication Element

This element (using vendor-specific information) enables the Cisco WLCs and mobile devices to indicate that they are HotSpot (HS) 2.0 capable. All the beacon and probe response frames from HS 2.0 Cisco WLCs contain this HS 2.0 indication element. For mobile devices, the association and re-association request frames contain the HS 2.0 indication element.

OSU Service Provider List

This element provides information for the entities offering OSU service. The following information is provided for each OSU provider:

- A friendly name (in one or more human languages)-Name of the OSU provider in human language, which matches the name drawn from the OSU server certificate exactly.
- The Network Access Identifier (NAI) used to authenticate to the OSU (if configured for OSEN).
- The icons and Uniform Resource Identifier (URI) of the OSU server.

Note The WLC supports a maximum of 16 service providers per OSU-SP list.

The Icon Request or Response ANQP Element

This element provides a filename for the (icon) download request from the mobile device, which is one of the filenames included in the OSU providers list element. The maximum file size for the icon is 65535 octets; the file type should be a valid image type, for example, PNG, JPEG, and so on. The file type restriction is not applicable for Cisco WLC and supports a maximum of 16 icons.

OSEN

The OSEN element is used to advertise and select an OSEN-capable network.

WNM Notification Subscription Remediation Request

The WNM notification request is sent from a WLC to a mobile device to indicate that subscription remediation is required when the AAA server indicates to WLC of this requirement through the RADIUS Access-Accept message. After the authentication is complete, the WLC sends WNM motification to the mobile device, using the URL of the Subscription Remediation server as the server URL.

WNM Notification Deauth Imminent Request

A home SP uses the Deauthentication Imminent Notice to inform the mobile device when it is no longer authorized to use the service due to a temporary condition in the network that requires deauthentication, for example, congestion in the Wi-Fi AN or congestion on a mobile core network element. The notice also provides information on the time that must elapse before the AAA server permits the mobile device to reauthenticate again on the same Basic Service Set (BSS) or Extended Service Set (ESS). Following this, the mobile device should not try to reauthenticate to the same BSS or ESS until the expiry of the reauthentication delay.

BSS Transition Management Request Frame - Session URL

The controller uses the BSS Transition Management Request frame to inform the mobile device of the impending session expiry. It also provides an URL to the user detailing on how to extend the session. The

controller gets the information about session warning time and URL from the AAA server through the Access-Accept message.

Extended Capability Bit Support

This element has two sections, WNM Notification and QoS Map Set, which are explained in the previous sections.

Configuring 802.11u Mobility Services Advertisement Protocol

Information About 802.11u MSAP

MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers.

Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.

Configuring 802.11u MSAP (GUI)

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

Step 2 Hover your mouse over the blue drop-down arrow for the desired WLAN on which you want to configure the MSAP parameters and select **Service Advertisements**. The Service Advertisement page appears.

Step 3 Enable the service advertisements.

Step 4 Enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.

Step 5 Click **Apply**.

Configuring MSAP (CLI)

- To enable or disable MSAP on a WLAN, enter this command:
  config wlan hotspot msap {**enable** | **disable**} *wlan-id*
- To assign a server ID, enter this command:
  config wlan hotspot msap server-id *server-id wlan-id*

Configuring 802.11u HotSpot

Information About 802.11u HotSpot

This feature, which enables IEEE 802.11 devices to interwork with external networks, is typically found in hotspots or other public networks irrespective of whether the service is subscription based or free.

The interworking service aids network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks prior to association. Interworking not only helps users within the home, enterprise, and public access, but also assists manufacturers and operators to provide common components and services for IEEE 802.11 customers. These services are configured on a per WLAN basis on the controller.

Note The Downstream Group-Addressed Forwarding (DGAF) bit in the Hotspot 2.0 IE will not be updated automatically until you disable and enable the WLAN.

Configuring 802.11u HotSpot (GUI)

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

Step 2 Hover your mouse over the blue drop-down arrow that corresponds to the desired WLAN on which you want to configure the HotSpot parameters and choose **HotSpot**. The **WLAN > HotSpot 2.0** page is displayed.

Step 3 On the **WLAN > HotSpot 2.0** window, enable HotSpot2.

Step 4 In the **Domain ID** field, enter the domain identifier.

Step 5 In the **OSU SSID** field, enter the OSU SSID.

Step 6 To set the WAN link parameters, perform the following tasks:

a) From the **WAN Link Status** drop-down list, choose the status. The default is the Not Configured status.
b) From the **WAN Symmetric Link Status** drop-down list, choose the status as either **Different** or **Same**.
c) Enter the **WAN Downlink and Uplink** speeds. The maximum value is 4,294,967,295 kbps.

Step 7 In the **Online Sign Up List** area, perform the following tasks:

a) From the **OSU Index** drop-down list, choose the OSU index you want to use.
b) From the **Lang Code** drop-down list, choose the language code you want to use, and select whether its in ASCII or HEX format from the next drop down list.
c) In the **SP Name** field, enter the service provider name.
d) In the **Description** field, enter the description.
e) Click **Add** to add the parameters to the list.

Step 8 In the **Operator Name List** area, perform the following tasks:

a) In the **Operator Name** text box, enter the name of the 802.11 operator.
b) From the **Operator index** drop-down list, choose an index value between 1 and 32 for the operator.

c) In the **Language Code** field, enter an ISO-14962-1997-encoded string defining the language. This string is a three-character language code.
d) Click **Add** to add the operator details.
The operator details are displayed in a tabular form. To remove an operator, hover your mouse pointer over the blue drop-down arrow and choose **Remove**.

Step 9 In the **Port Config List** area, perform the following tasks:

a) From the **IP Protocol** drop-down list, choose the IP protocol that you want to enable.
b) From the **Port No** drop-down list, choose the port number that is enabled on the WLAN.
c) From the **Status** drop-down list, choose the status of the port.
d) From the **Index** drop-down list, choose an index value for the port configuration.
e) Click **Add** to add the port configuration parameters.
To remove a port configuration list, hover your mouse over the blue drop-down arrow and choose **Remove**.

Step 10 Click **Apply**.

Configuring HotSpot 2.0 (CLI)

Note The character '?' is not supported in the value part of the commands.

- To enable or disable HotSpot2 on a WLAN, enter this command:

  config wlan hotspot hs2 {**enable** | **disable**}

- To configure the operator name on a WLAN, enter this command:

  config wlan hotspot hs2 operator-name {**add** | **modify**} *wlan-id index operator-name lang-code*

  The following options are available:

  - *wlan-id*—The WLAN ID on which you want to configure the operator-name.
  - *index*—The operator index of the operator. The range is 1 to 32.
  - *operator-name*—The name of the 802.11an operator.
  - *lang-code*—The language used. An ISO-14962-1997 encoded string defining the language. This string is a three character language code. Enter the first three letters of the language in English (For example: eng for English).

    Tip Press the tab key after entering a keyword or argument to get a list of valid values for the command.

- To delete the operator name, enter this command:

  config wlan hotspot hs2 operator-name delete *wlan-id index*

- To configure the port configuration parameters, enter this command:

  config wlan hotspot hs2 port-config {**add** | **modify**} *wlan-id index ip-protocol port-number*

- To delete a port configuration, enter this command:

  config wlan hotspot hs2 port-config delete *wlan-id index*

- To configure the WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics *wlan-id link-status symet-link downlink-speed uplink-speed*

  The values are as follows:

  - *link-status*—The link status. The valid range is 1 to 3.
  - *symet-link*—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
  - *downlink-speed*—The downlink speed. The maximum value is 4,194,304 kbps.
  - *uplink-speed*—The uplink speed. The maximum value is 4,194,304 kbps.

- To clear all HotSpot configurations, enter this command:

  config wlan hotspot clear-all *wlan-id*

- To configure the Access Network Query Protocol (ANQP) 4-way messaging, enter this command:

  config advanced hotspot anqp-4way {**enable** | **disable** | **threshold** *value*}

- To configure the ANQP comeback delay value in terms of TUs, enter this command:

  config advanced hotspot cmbk-delay *value*

- To configure the gratuitous ARP (GARP) forwarding to wireless networks, enter this command:

  config advanced hotspot garp {**enable** | **disable**}

- To limit the number of GAS request action frames to be sent to the controller by an AP in a given interval, enter this command:

  config advanced hotspot gas-limit {**enable** *num-of-GAS-required interval* | **disable**}

Configuring Access Points for HotSpot2 (GUI)

When HotSpot2 is configured, the access points that are part of the network must be configured to support HotSpot2.

Step 1 Click **Wireless > All APs** to open the All APs page.

Step 2 Click the **AP Name** link to configure the HotSpot parameters on the desired access point. The AP Details page appears.

Step 3 Under the General Tab, configure the following parameters:

- **Venue Group**—The venue category that this access point belongs to. The following options are available:
  - **Unspecified**
  - **Assembly**

- **Business**
- **Educational**
- **Factory and Industrial**
- **Institutional**
- **Mercantile**
- **Residential**
- **Storage**
- **Utility and Misc**
- **Vehicular**
- **Outdoor**

- **Venue Type—**Depending on the venue category selected above, the venue type drop-down list displays options for the venue type.
- **Venue Name—**Venue name that you can provide to the access point. This name is associated with the BSS. This is used in cases where the SSID does not provide enough information about the venue.
- **Language—**The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (For example, eng for English).

Step 4 Click **Apply**.

Configuring Access Points for HotSpot2 (CLI)

- **config ap venue add** *venue-name venue-group venue-type lang-code ap-name***–**Adds the venue details to the access point indicating support for HotSpot2.

  The values are as follows:

  - *venue-name***—**Name of the venue where this access point is located.
  - *venue-group***—**Category of the venue. See the following table.
  - *venue-type***—**Type of the venue. Depending on the venue-group chosen, select the venue type. See the following table.
  - *lang-code***—**The language used. An ISO-14962-1997 encoded string defining the language. This is a three character language code. Enter the first three letters of the language in English (For example: eng for English)
  - *ap-name***—**Access point name.

Tip Press the tab key after entering a keyword or argument to get a list of valid values for the command.

- **config ap venue delete** *ap-name*—Deletes the venue related information from the access point.

Table 1: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	
ASSEMBLY	1	• 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 4—AMPHITHEATER • 5—AMUSEMENT PARK • 6—PLACE OF WORSHIP • 7—CONVENTION CENTER • 8—LIBRARY • 9—MUSEUM • 10—RESTAURANT • 11—THEATER • 12—BAR • 13—COFFEE SHOP • 14—ZOO OR AQUARIUM • 15—EMERGENCY COORDINATION CENTER

Venue Group Name	Value	Venue Type for Group
BUSINESS	2	• 0—UNSPECIFIED BUSINESS • 1—DOCTOR OR DENTIST OFFICE • 2—BANK • 3—FIRE STATION • 4—POLICE STATION • 6—POST OFFICE • 7—PROFESSIONAL OFFICE • 8—RESEARCH AND DEVELOPMENT FACILITY • 9—ATTORNEY OFFICE
EDUCATIONAL	3	• 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE
FACTORY-INDUSTRIAL	4	• 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY
INSTITUTIONAL	5	• 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL

Venue Group Name	Value	Venue Type for Group
MERCANTILE	6	• 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION
RESIDENTIAL	7	• 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE
STORAGE	8	UNSPECIFIED STORAGE
UTILITY-MISC	9	0—UNSPECIFIED UTILITY AND MISCELLANEOUS
VEHICULAR	10	• 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE

Venue Group Name	Value	Venue Type for Group
OUTDOOR	11	• 0—UNSPECIFIED OUTDOOR • 1—MUNI-MESH NETWORK • 2—CITY PARK • 3—REST AREA • 4—TRAFFIC CONTROL • 5—BUS STOP • 6—KIOSK

Downloading the Icon File (CLI)

You can configure unique icons of the service providers to be displayed on the client devices. You can download these icon files to the Cisco WLC for the icon files to be sent through a gas message and displayed on the client devices. This feature enhances the user interface on the client devices wherein users can differentiate between service providers based on the icons displayed.

Step 1 Save the icon file on an TFTP, SFTP, or an FTP server.

Step 2 Download the icon file to the Cisco WLC by entering these commands:

a) **transfer download datatype icon**

b) **transfer download start**

Configuring ICONs

Note The character '?' is not supported in the command values.

- To download an icon from the TFTP server or FTP server into Cisco Wireless Controller (WLC), enter this command:

  configure icon parameters

- To configure icon parameters, enter this command:

  config icons file-info *filename file-type lang-code width height*

- To delete an icon from flash, enter this command:

  config icons delete {*filename* | **all**}

- To display icon parameters, enter this command:

  show icons summary

Downloading an ICON File (GUI)

Step 1 Copy the **ICON** file to the default directory on your server.

Step 2 Choose **Commands > Download File**.
The **Download File to Controller** window is displayed.

Step 3 From the **File Type** drop-down list, choose ICON.

Step 4 From the **Transfer Mode** drop-down list, choose from one of the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in Release 7.4 and later releases)

Step 5 In the **IP Address** field, enter the IP address of the server type you chose in Step 4. If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout fields should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times the TFTP server can attempt to download the certificate in the Maximum Retries text box, and the amount of time (in seconds) that the TFTP server can attempt to download the certificate in the **Timeout** field.

Step 7 In the **File Path** field, enter the directory path of the icon file.

Step 8 In the **File Name** field, enter the name of the icon file.

Step 9 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** text box, enter the username to log in to the FTP server.
b) In the **Server Login Password** text box, enter the password to log in to the FTP server.
c) In the **Server Port Number** text box, enter the port number in the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the login ICON file to the Cisco Wireless Controller (WLC).
A message is displayed indicating the status of the download.

Step 11 Click **Apply**.

Configuring an ICON (GUI)

Step 1 Choose **Controller > Icons**.
The **Icon Configuration** window is displayed.

Step 2 In the **Filename** field, enter the filename for the icon.
Step 3 In the **File Type** field, enter the file type of the icon.
Step 4 In the **Lang Code** field, enter the language code.
Step 5 In the **Width** field, enter the width of the icon.
Step 6 In the **Height** field, enter the height of the icon.
Step 7 Click **Add**.
Step 8 Click **Apply**.

Configuring OSEN Support

Note The character '?' is not supported in the command values.

- To enable or disbale OSEN on a given WLAN, enter this command:
  config wlan security wpa osen {**enable** | **disable**} *wlan-id*
- To display OSEN details on a given WLAN, enter this command:
  show wlan *wlan-id*

Configuring OSEN Details (GUI)

Step 1 Choose **WLAN** to open the **WLANs** window.
Step 2 Click the WLAN ID to open the Edit page pertaining to the selected WLAN.
Step 3 Click the **Security** tab and then the **Layer 2** tab.
Step 4 From the **Layer 2 Security** drop-down list, choose **WPA+WPA2**.
Step 5 Under **WPA+WPA2 Parameters**, check the **OSEN Policy** check box to enable OSEN.
Step 6 Check the **OSEN Encryption** check box to enable OSEN encryption, and check the **TKIP** check box to enable TKIP.
Step 7 Click **Apply**.

Configuring OSU

Note The character '?' is not supported in the command values.

- To configure an (OSU) Service Set Identifier (SSID) name, enter this command:

  config wlan hotspot hs2 osu legacy-ssid {**wlan-id** | **ssid-name**}

- To create an OSU service provider name, enter this command:

  config wlan hotspot hs2 osu sp create *wlan-id osu-index lang-code ascii/hex friendly-name*[*description*]

  The following options are available:

  - *wlan-id*—The WLAN ID on which you want to configure the operator-name.
  - *osu-index*—The osu index of the operator. The range is 1 to 32.
  - *lang-code*—The language used.
  - *ascii/hex*—.
  - *friendly-name*—The name of the 802.11an operator.
  - *description*—The language used.

- To delete an OSU service provider, enter this command:

  config wlan hotspot hs2 osu sp delete *wlan-id osu-index lang-code*

- To configure a domain ID, enter this command:

  config wlan hotspot hs2 domain-id {**wland** | **domain-id**}

- To create an OSU URL, enter this command:

  config wlan hotspot hs2 osu sp uri add *wlan-id osu-index uri*

- To delete an OSU URL, enter this command:

  config wlan hotspot hs2 osu sp uri delete *wlan-id osu-index*

- To configure an OSU method list, enter this command:

  config wlan hotspot hs2 osu sp method add *wlan-id osu-index method-pri* [*method-sec*]

- To delete an OSU method list, enter this command:

  config wlan hotspot hs2 osu sp method delete *wlan-id osu-index method*

- To configure an OSU icon file on a given WLAN, enter this command:

  config wlan hotspot hs2 osu sp icon-file add *wlan-id osu-index icon-filename*

Note Yous should first configure icon parameters using the **config icon** *icon-filename* command.

- To delete an OSU icon file from a given WLAN, enter this command:

  config wlan hotspot hs2 osu sp icon-file delete *wlan-id osu-index icon-filename*

- To configure an OSU NAI, enter this command:

  config wlan hotspot hs2 osu sp nai add *wlan-id osu-index nai*

- To delete an OSU NAI, enter this command:

config wlan hotspot hs2 osu sp nai delete *wlan-id osu-index*

- To display the OSU details configured on a given WLAN, enter this command:

  show wlan *wlan-id*

Configuring OSU Details (GUI)

Step 1 Choose **WLAN**.
It opens the WLANs window.

Step 2 Hover your mouse over the blue drop-down arrow corresponding to the desired WLAN on which you want to configure the OSU parameters and choose **802.11u**.
The **802.11u Parameters** window appears.

Step 3 In the **WLAN > 802.11u Parameters** window, enable 802.11u.

Step 4 In the Service Provider Name field, enter the name of the service provider.
The **OSU Index** field displays the OSU index that you are editing.

The **Language Code** field displays the language code associated with the OSU Index.

Step 5 In the **Description** field, enter the description for the OSU.

Step 6 In the **URI** field, enter the URI details.

Step 7 In the **NAI** field, enter the NAI details.

Step 8 In the **Icon Filename** field, enter the filename for the icon associated with the service provider.

Step 9 From the **Method** drop-down list, choose the association method.

Step 10 Click **Apply**.

Configuring WAN Metrics

Note The character '?' is not supported in the command values.

- To configure downlink WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics downlink *wlan-id dlink-speed dlink-load*

- To configure uplink WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics uplink *wlan-id ulink-speed ulink-load*

- To configure the link status of WAN metrics, enter this command:

  config wlan hotspot hs2 wan-metrics link-status *wlan-id link-status*

- To configure the load measurement duration WAN metrics, enter this command:

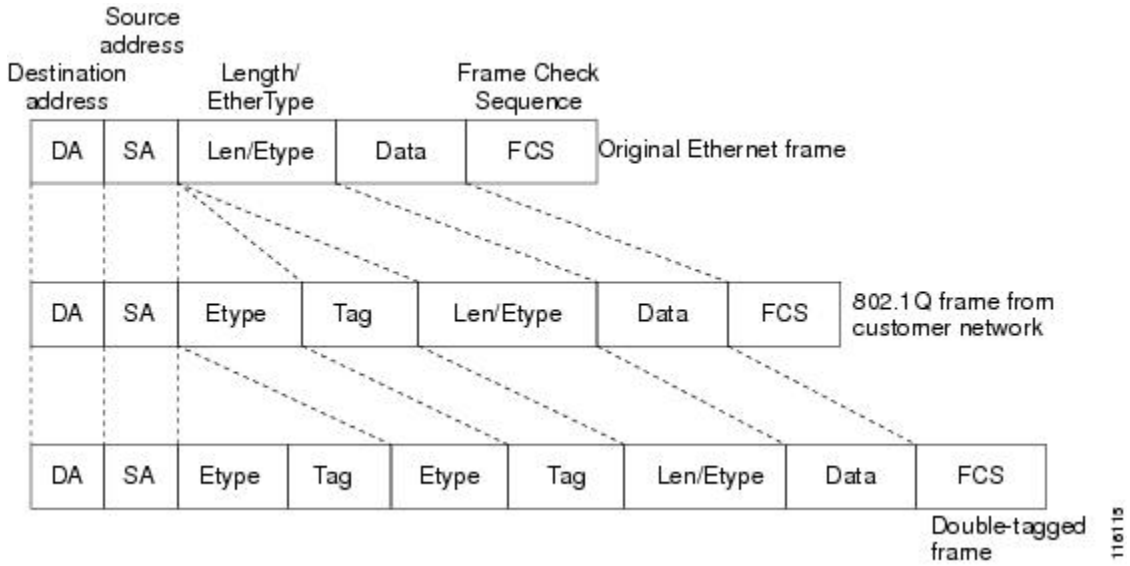
  config wlan hotspot hs2 wan-metrics lmd *wlan-id ilmd-val*

Information About 802.1Q-in-Q VLAN Tagging

Assigning a unique range of VLAN IDs to each client can exceed the limit of 4096 VLANs. The 802.1Q-in-Q VLAN tag feature encapsulates the 802.1Q VLAN tagging within another 802.1Q VLAN tag. The outer tag is assigned according to the AP group, and the inner VLAN ID is assigned dynamically by the AAA server.

Using the 802.1Q-in-Q feature you can use a single VLAN to support multiple VLANs. With the 802.1Q-in-Q feature you can preserve VLAN IDs and segregate traffic of different VLANs. The figure below shows the untagged, 802.1Q-tagged, and 802.1Q-in-Q tagged Ethernet frames.

Figure 1: Untagged 802.1Q-Tagged and 802.1Q-in-Q Tagged Ethernet Frames



Related Topics

Configuring 802.1Q-in-Q VLAN Tagging (GUI), on page 20
Configuring 802.1Q-in-Q VLAN Tagging (CLI), on page 20
Restrictions for 802.1Q-in-Q VLAN Tagging, on page 19

Configuring 802.1Q-in-Q VLAN Tagging (GUI), on page 20
Configuring 802.1Q-in-Q VLAN Tagging (CLI), on page 20
Restrictions for 802.1Q-in-Q VLAN Tagging, on page 19

Restrictions for 802.1Q-in-Q VLAN Tagging

- 802.1Q-in-Q VLAN tagging is supported only on Cisco 5500 Series Wireless LAN Controllers, Cisco 8500 Series Wireless LAN Controllers, and Cisco WiSM2.
- You cannot enable multicast until you disable IGMP snooping.
- 802.1Q-in-Q VLAN tagging is supported only on Layer 2 and Layer 3 intra-Controller roaming, and Layer 2 inter-Controller roaming. Layer 3 inter-Controller roaming is not supported.

- 0x8100 is the only supported value for the EtherType field of the 802.1Q-in-Q Ethernet frame.
- You can enable 802.1Q-in-Q VLAN tagging only on centrally switched packets.
- You can enable only IPv4 DHCP packets and not IPv6 DHCP packets for 802.1Q-in-Q VLAN tagging.
- The IETF attribute which is a tunnel-type is required to override the C-VLAN.
- C-VLAN can be set with tunnel-private-group-ID /tunnel-type and tunnel-private-group-id.

Related Topics

Information About 802.1Q-in-Q VLAN Tagging, on page 19
Configuring 802.1Q-in-Q VLAN Tagging (GUI), on page 20
Configuring 802.1Q-in-Q VLAN Tagging (CLI), on page 20
Information About 802.1Q-in-Q VLAN Tagging, on page 19
Configuring 802.1Q-in-Q VLAN Tagging (GUI), on page 20
Configuring 802.1Q-in-Q VLAN Tagging (CLI), on page 20

Configuring 802.1Q-in-Q VLAN Tagging (GUI)

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** to open the AP Groups page.
Step 2 Click an AP group Name to open the corresponding AP Group > Edit page.
Step 3 Click the **General** tab to configure the 802.1Q-in-Q VLAN tagging details.
Step 4 Select the **Enable Client Traffic QinQ** check box to enable 802.1Q-in-Q VLAN tagging for the AP group.
Step 5 Select the **Enable DHCPv4 QinQ** check box to enable 802.1Q-in-Q VLAN tagging of IPv4 DHCP packets in the AP group.
Step 6 In the **QinQ Service VLAN ID** text box, enter the VLAN ID for 802.1Q-in-Q VLAN tagging.
Step 7 Click **Apply**.

Related Topics

Information About 802.1Q-in-Q VLAN Tagging, on page 19
Restrictions for 802.1Q-in-Q VLAN Tagging, on page 19
Information About 802.1Q-in-Q VLAN Tagging, on page 19
Restrictions for 802.1Q-in-Q VLAN Tagging, on page 19

Configuring 802.1Q-in-Q VLAN Tagging (CLI)

Step 1 Enable or disable 802.1Q-in-Q VLAN tagging for an AP group by entering this command:
config wlan apgroup qinq tagging client-traffic *apgroup_name* {**enable** | **disable**}

By default, 802.1Q-in-Q tagging of client traffic for an AP group is disabled.

Step 2 Configure the service VLAN for the AP group by entering this command:
config wlan apgroup qinq service-vlan *apgroup_name vlan_id*

Step 3 Enable or disable IPv4 DHCP packets of the client traffic in the AP group by entering this command::
config wlan apgroup qinq tagging dhcp-v4 *apgroup_name* {**enable** | **disable**}

Note You must enable 802.1Q-in-Q tagging of client traffic before you enable 802.1Q-in-Q tagging of DHCPv4 traffic.

By default, 802.1Q-in-Q tagging of DHCPv4 traffic for an AP group is disabled.

Step 4 Enable or disable 802.1Q-in-Q VLAN tagging for EAP for Global System for Mobile Communications (GSM) Subscriber Identity Module (EAP-SIM) or EAP for Authentication and Key Agreement-authenticated client traffic in the AP group by entering this command:
config wlan apgroup qinq tagging eap-sim-aka *apgroup_name* {**enable** | **disable**}

When you enable 802.1Q-in-Q tagging of client traffic, the 802.1Q-in-Q tagging of EAP for Authentication and Key Agreement (EAP-AKA) and EAP-SIM traffic is enabled.

Step 5 Verify if 802.1Q-in-Q VLAN tagging is enabled by entering this command:
show wlan apgroups

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..................... 5


Site Name..................................... CT_builing1
Site Description.............................. APs for CT Building1
Venue Group Code.............................. Unspecified
Venue Type Code............................... Unspecified

NAS-identifier................................ CTB1
Client Traffic QinQ Enable.................... TRUE
DHCPv4 QinQ Enable............................ TRUE
AP Operating Class............................ Not-configured
```

Related Topics

Information About 802.1Q-in-Q VLAN Tagging, on page 19
Restrictions for 802.1Q-in-Q VLAN Tagging, on page 19
Information About 802.1Q-in-Q VLAN Tagging, on page 19
Restrictions for 802.1Q-in-Q VLAN Tagging, on page 19