Per-WLAN Wireless Settings

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 broadcast and multicast frames 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 for 10 times every 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 for 5 times every 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). The only recommended DTIM values are 1 and 2; higher DTIM values will likely cause communications problems.

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. Depending on the AP model, the actual beacon period may vary slightly; for example, a beacon period of 100 ms may in practice equate to 104.448 ms.

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.

This section contains the following subsections:

Configuring the DTIM Period (GUI)

Procedure

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	Uncheck 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	Check the **Status** check box to reenable the WLAN.
Step 10	Click **Save Configuration**.

Configuring the DTIM Period (CLI)

Procedure

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*

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.

For more information about CCX Lite, see
http://www.cisco.com/c/en/us/products/wireless/compatible-extensions.html

This section contains the following subsections:

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.

Guidelines and Restrictions for Configuring Cisco Client Extensions

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

- Cisco OEAP 600 do not support Cisco Aironet IEs.

Configuring CCX Aironet IEs (GUI)

Procedure

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   Check 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.

Procedure

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*

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 profiling is enabled.

Controller has been enhanced with some of these following capabilities:

- Controller 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.

- Controller 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

Information about Custom HTTP Port Profiling

This feature is designed to enable the controller to identify and profile clients connecting from ports apart from HTTP port 80.

This section contains the following subsections:

Prerequisites for Configuring Client Profiling

- By default, client profiling will be disabled on all WLANs.

- Client profiling is supported on access points that are in Local mode and FlexConnect mode.

- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.

- Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.

- The type of DHCP server used does not affect client profiling.

- If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.

- The client is identified based on the MAC address sent in the Accounting request packet.

- Only a MAC address should be sent as calling station ID in accounting packets when profiling is enabled.

- To enable client profiling, you must enable the DHCP required flag and disable the local authentication flag.

- Client profiling uses pre-existing profiles in the controller.

- Profiling for Wireless clients are done based on MAC OUI, DHCP, HTTP User agent.

Note DHCP is required for DHCP profiling and Webauth for HTTP user agent.

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.

- When local profiling is enabled, RADIUS profiling is not allowed on a 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 occur 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 because the AAA override attributes have a higher precedence.

- For Apple devices, the version and operating system information is displayed only for iPhone 7 and later models and iPads introduced in 2017 and later, provided the WLAN is not open. The version and operating system information is not displayed for older devices.

- This feature supports HTTP profiling based on custom HTTP port and only one custom HTTP port can be configured.

Configuring Client Profiling (GUI)

Procedure

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 **RADIUS and Local Client Profiling** area, do the following:

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

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

You can configure client profiling in both RADIUS mode and Local mode on the WLAN.

Step 5   Click **Apply**.

Step 6   Click **Save Configuration**.

Configuring Client Profiling (CLI)

• Enable or disable client profiling for a WLAN based on DHCP by entering this command:

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

• 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.

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

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

• 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 Custom HTTP Port for Profiling (GUI)

Note   The HTTP port 80 is always open for gathering HTTP profiling data, irrespective of the custom HTTP port configuration.

Procedure

Step 1   Choose **Controller** > **General** to open the general page.

Step 2   Enter the port value under **HTTP Profiling Port** field.

Configuring Custom HTTP Port for Profiling (CLI)

Procedure

Step 1 Configure custom HTTP port by entering this command:

config network profiling http-port *port number*

The default port value is 80.

Step 2 View the configured HTTP profiling port and other inband connectivity settings by entering this command:

show network summary

The network configuration is displayed.

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 3000 total clients and these clients can be shared between enterprise users (employees) and guest users, so you can limit the guest WLAN to 500 clients. The number of clients that you can configure for each WLAN depends on the platform that you are using. Additionally, you can set a limit on the number of clients in a given WLAN that can associate to each AP's radio. For example, each radio supports up to 200 associations, but a guest WLAN may be configured for a maximum of 10 associations per radio.

This section contains the following subsections:

Restrictions for Setting Client Count for WLANs

- 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)

Procedure

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)

Procedure

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)

Procedure

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)

Procedure

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.

Limit Clients per WLAN per AP Radio

Limit Clients per WLAN per AP Radio (GUI)

- With the AP in Local mode, Cisco WLC validates the association request of all clients. Cisco WLC drops a client association request if the configured limit has been reached.

- With the AP in FlexConnect mode, both connected (local or central switching, local or central authentication) and standalone mode (local switching, local authentication), the AP validates the client admission in the authentication or reassociation phase.

Procedure

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

Step 2   Click the WLAN ID.

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

Step 4   In the **Maximum Allowed Clients** field, enter the maximum number of clients that can be allowed to join the WLAN.

Note   If you enter a value of 0, this means that there is no restriction on the number of clients that are allowed to join the WLAN.

Step 5   In the **Maximum Allowed Clients Per AP Radio** field, enter the maximum number of clients that can be allowed to join the WLAN per AP radio.

Valid range is between 1 to 200 clients.

Step 6   Save the configuration.

Limit Clients per WLAN per AP Radio (CLI)

- With the AP in Local mode, Cisco WLC validates the association request of all clients. Cisco WLC drops a client association request if the configured limit has been reached.

- With the AP in FlexConnect mode, both connected (local or central switching, local or central authentication) and standalone mode (local switching, local authentication), the AP validates the client admission in the authentication or reassociation phase.

Procedure

Step 1   Configure the maximum number of clients that can be allowed to join the WLAN per AP radio by entering this command:

config wlan max-radio-clients *max-clients wlan-id*

Step 2   View the client information by entering these commands:

- On the Cisco WLC console—**show client summary**
- On the Cisco Wave 2 AP console—**show dot11 clients**

Step 3   Enable debugging on the Cisco Wave 2 AP console by entering these commands:

- Enable 802.11 event level debugging—**debug dot11 events**

- Enable 802.11 information level debugging—**debug dot11 info**

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.

This section contains the following subsections:

Disabling Coverage Hole Detection on a WLAN (GUI)

Procedure

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   Uncheck 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)

Procedure

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
```