Configuring Client Roaming

Information About Client Roaming

The Cisco UWN solution supports seamless client roaming across lightweight access points managed by the same controller, between controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on different subnets. Also, in controller software release 4.1 or later releases, client roaming with multicast packets is supported.

You can adjust the default RF settings (RSSI, hysteresis, scan threshold, and transition time) to fine-tune the operation of client roaming using the controller GUI or CLI.

Intra-Controller Roaming

Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address. The controller provides DHCP functionality with a relay function. Same-controller roaming is supported in single-controller deployments and in multiple-controller deployments.

Inter-Controller Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client because the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set session timeout is exceeded.

Inter-Subnet Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set user timeout is exceeded.

Voice-over-IP Telephone Roaming

802.11 voice-over-IP (VoIP) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VoIP telephone requirement of 20-millisecond or shorter latency time for the roaming handover is easily met by the Cisco Wireless solution, which has an average handover latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiate roaming handovers.

The Cisco Wireless solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP address as long as the session remains active. The tunnel is torn down, and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP address or a 169.254.*.* VoIP telephone auto-IP address or when the operator-set user timeout is exceeded.

CCX Layer 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.

- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.

- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.

| **Note** | To see whether a particular client supports E2E, choose **Wireless** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the E2E Version text box in the Client Properties area. |

- Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.

- Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

This section contains the following subsections:

Restrictions for Client Roaming

- CCX versions 1 through 5 are supported. 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 generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) in order to utilize these roaming enhancements.

  The roaming enhancements mentioned above are enabled automatically, with the appropriate CCX support.

- FlexConnect access points in standalone mode do not support CCX Layer 2 roaming.

- Client roaming between Cisco 600 Series OEAPs is not supported.

- Seamless L2 and L3 roaming is not supported between a Cisco and a third-party wireless infrastructure, which also includes a Cisco IOS access point.

Configuring CCX Client Roaming Parameters (GUI)

Step 1 Choose **Wireless** > **802.11a/n or 802.11b/g/n** > **Client Roaming**. The 802.11a (802.11b) > Client Roaming page appears.

Step 2 If you want to fine-tune the RF parameters that affect client roaming, choose **Custom** from the **Mode** drop-down list and go to *Step 3*. If you want to leave the RF parameters at their default values, choose **Default** and go to *Step 8*.

Step 3 In the **Minimum RSSI** text box, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.

The range is –90 to –50 dBm.

The default is –85 dBm.

Step 4   In the **Hysteresis** text box, enter a value to indicate how much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.

The range is 3 to 20 dB.

The default is 3 dB.

Step 5   In the **Scan Threshold** text box, enter the minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold.

The range is −90 to −50 dBm.

The default is −72 dBm.

Step 6   In the **Transition Time** text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.

The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

The range is 1 to 5 seconds.

The default is 5 seconds.

Step 7   Click **Apply**.

Step 8   Click **Save Configuration**.

Step 9   Repeat this procedure if you want to configure client roaming for another radio band.

Configuring CCX Client Roaming Parameters (CLI)

Configure CCX Layer 2 client roaming parameters by entering this command:

config {**802.11a** | **802.11b**} **l2roam rf-params** {**default** | **custom** *min_rssi roam_hyst scan_thresh trans_time*}

Obtaining CCX Client Roaming Information (CLI)

Step 1   View the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network by entering this command:

show {**802.11a** | **802.11b**} **l2roam rf-param**

Step 2   View the CCX Layer 2 client roaming statistics for a particular access point by entering this command:

show {**802.11a** | **802.11b**} **l2roam statistics** *ap_mac*

This command provides the following information:

- The number of roam reason reports received

- The number of neighbor list requests received

- The number of neighbor list reports sent

- The number of broadcast neighbor updates sent

Step 3   View the roaming history for a particular client by entering this command:

show client roam-history *client_mac*

This command provides the following information:

- The time when the report was received

- The MAC address of the access point to which the client is currently associated

- The MAC address of the access point to which the client was previously associated

- The channel of the access point to which the client was previously associated

- The SSID of the access point to which the client was previously associated

- The time when the client disassociated from the previous access point

- The reason for the client roam

Note   For non-CCXv4 clients, the Layer 2 roam reason is not displayed in the command output. For more information, see CSCvv85022.

Debugging CCX Client Roaming Issues (CLI)

If you experience any problems with CCX Layer 2 client roaming, enter this command:

debug l2roam [**detail** | **error** | **packet** | **all**] {**enable** | **disable**}