Auto-Anchor Mobility

Information about Auto-Anchor Mobility

You can use auto-anchor mobility (also called guest tunneling) to improve load balancing and security for roaming clients on your wireless LANs. Under normal roaming conditions, client devices join a wireless LAN and are anchored to the first controller that they contact. If a client roams to a different subnet, the controller to which the client roamed sets up a foreign session for the client with the anchor controller. However, when you use the auto-anchor mobility feature, you can specify a controller or set of controllers as the anchor points for clients on a wireless LAN.

In auto-anchor mobility mode, a subset of a mobility group is specified as the anchor controllers for a WLAN. You can use this feature to restrict a WLAN to a single subnet, regardless of a client's entry point into the network. Clients can then access a guest WLAN throughout an enterprise but still be restricted to a specific subnet. Auto-anchor mobility can also provide geographic load balancing because the WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on), effectively creating a set of home controllers for a WLAN. Instead of being anchored to the first controller that they happen to contact, mobile clients can be anchored to controllers that control access points in a particular vicinity.

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the client is announced to the other controllers in the mobility list. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

If multiple controllers are added as mobility anchors for a particular WLAN on a foreign controller, the foreign controller internally sorts the controller by their IP address. The controller with the lowest IP address is the first anchor. For example, a typical ordered list would be 172.16.7.25, 172.16.7.28, 192.168.5.15. If the first client associates to the foreign controller's anchored WLAN, the client database entry is sent to the first anchor controller in the list, the second client is sent to the second controller in the list, and so on, until the end of the anchor list is reached. The process is repeated starting with the first anchor controller. If any of the anchor controller is detected to be down, all the clients anchored to the controller are deauthenticated, and the clients then go through the authentication/anchoring process again in a round-robin manner with the remaining controller in the anchor list. This functionality is also extended to regular mobility clients through mobility failover. This feature enables mobility group members to detect failed members and reroute clients.

Restrictions for Auto-Anchor Mobility

- Mobility list members can send ping requests to one another to check the data and control paths among them to find failed members and reroute clients. You can configure the number and interval of ping requests that are sent to each anchor controller. This functionality provides guest N+1 redundancy for guest tunneling and mobility failover for regular mobility.
- You must add controllers to the mobility group member list before designating them as mobility anchors for a WLAN.
- Auto-anchor mobility does not support multiple WLANs with the same SSID name and WLAN ID used is number 17 or higher.
- You can configure multiple controllers as mobility anchors for a WLAN.
- You must configure the WLANs on both the foreign controller and the anchor controller with mobility anchors. On the anchor controller, configure the anchor controller itself as a mobility anchor. On the foreign controller, configure the anchor as a mobility anchor.
- It is not possible for clients, WGB, and wired clients to directly connect to a DMZ guest anchor and move to a foreign controller.
- Auto-anchor mobility is not supported for use with DHCP option 82.
- When using the guest N+1 redundancy and mobility failover features with a firewall, make sure that the following ports are open:
  - UDP 16666 for tunnel control traffic
  - IP Protocol 97 for user data traffic
  - UDP 161 and 162 for SNMP
- In case of roaming between anchor controller and foreign mobility, the client addresses learned at the anchor controller is shown at the foreign controller. You must check the foreign controller to view the RA throttle statistics.
- For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.
- The mobility anchor is not supported on virtual wireless LAN controllers.
- In a guest anchor Cisco WLC deployment, ensure that the foreign Cisco WLC does not have a WLAN mapped to a VLAN that is associated with the guest anchor Cisco WLC.

- In Old Mobility, when roaming from foreign to anchor WLC, the other foreign WLCs in the mobility group do not receive mobile announce messages.

Configuring Auto-Anchor Mobility (GUI)

Procedure

Step 1 Configure the controller to detect failed anchor controllers within a mobility group as follows:

a) Choose **Controller** > **Mobility Management** > **Mobility Anchor Config** to open the Mobility Anchor Config page.

b) In the Keep Alive Count text box, enter the number of times a ping request is sent to an anchor controller before the anchor is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.

c) In the Keep Alive Interval text box, enter the amount of time (in seconds) between each ping request that is sent to an anchor controller. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

Note We recommend that you use the default keepalive count and interval values to reduce converge time between the Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers while setting up a mobility tunnel.

d) In the DSCP Value text box, enter the DSCP value. The default is 0.

Note While configuring the Mobility DSCP value, the mobility control socket (i.e control messages exchanged between mobility peers only and not the data) is also updated. The configured value must reflect in the IPV4 header TOS field. This is a global configuration on the controller that is used to communicate among configured mobility peers only.

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

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

Step 3 Click the blue drop-down arrow for the desired WLAN or wired guest LAN and choose **Mobility Anchors**. The Mobility Anchors page appears.

This page lists the controllers that have already been configured as mobility anchors and shows the current state of their data and control paths. Controllers within a mobility group communicate among themselves over a well-known UDP port and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. They send mpings, which test mobility control packet reachability over the management interface over mobility UDP port 16666 and they send epings, which test the mobility data traffic over the management interface over EoIP port 97. The Control Path text box shows whether mpings have passed (up) or failed (down), and the Data Path text box shows whether epings have passed (up) or failed (down). If the Data or Control Path text box shows “down,” the mobility anchor cannot be reached and is considered failed.

Step 4 Select the IPv4/IPv6 address of the controller to be designated a mobility anchor in the Switch IP Address (Anchor) drop-down list.

Step 5 Click **Mobility Anchor Create**. The selected controller becomes an anchor for this WLAN or wired guest LAN.

Note To delete a mobility anchor for a WLAN or wired guest LAN, hover your cursor over the blue drop-down arrow for the anchor and choose **Remove**.

Step 6 Click **Save Configuration**.

Step 7 Repeat *Step 4* and *Step 6* to set any other controllers as mobility anchors for this WLAN or wired guest LAN.

Step 8 Configure the same set of mobility anchors on every controller in the mobility group.

Configuring Auto-Anchor Mobility (CLI)

Procedure

Step 1 The controller is programmed to always detect failed mobility list members. To change the parameters for the ping exchange between mobility members, enter these commands:

- **config mobility group keepalive count** *count*—Specifies the number of times a ping request is sent to a mobility list member before the member is considered to be unreachable. The valid range is 3 to 20, and the default value is 3.
- **config mobility group keepalive interval** *seconds*—Specifies the amount of time (in seconds) between each ping request sent to a mobility list member. The valid range is 1 to 30 seconds, and the default value is 10 seconds.

Note We recommend that you use the default keepalive count and interval values to reduce converge time between the Cisco AireOS Wireless Controllers and Cisco Catalyst 9800 Series Wireless Controllers while setting up a mobility tunnel.

Step 2 Disable the WLAN or wired guest LAN for which you are configuring mobility anchors by entering this command:

config {wlan | guest-lan} disable {*wlan_id* | *guest_lan_id*}

Step 3 Create a new mobility anchor for the WLAN or wired guest LAN by entering one of these commands:

- **config mobility group anchor add** {**wlan | guest-lan**} {*wlan_id* | *guest_lan_id*} *anchor_controller_ip_address*
- **config** {**wlan | guest-lan**} **mobility anchor add** {*wlan_id* | *guest_lan_id*} *anchor_controller_ip_address*

Note The *wlan_id* or *guest_lan_id* must exist and be disabled, and the *anchor_controller_ip_address* must be a member of the default mobility group.

Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor.

Step 4 Delete a mobility anchor for the WLAN or wired guest LAN by entering one of these commands:

- **config mobility group anchor delete {wlan | guest-lan} {wlan_id | guest_lan_id}** anchor_controller_ip_address
- **config {wlan | guest-lan} mobility anchor delete {wlan_id | guest_lan_id}** anchor_controller_ip_address

Note The *wlan_id* or *guest_lan_id* must exist and be disabled.

Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

Step 5 Save your settings by entering this command:

save config

Step 6 See a list and status of controllers configured as mobility anchors for a specific WLAN or wired guest LAN by entering this command:

show mobility anchor {**wlan** | *guest-lan*} {*wlan_id* | *guest_lan_id*}

Note The *wlan_id* and *guest_lan_id* parameters are optional and constrain the list to the anchors in a particular WLAN or guest LAN. To see all of the mobility anchors on your system, enter the **show mobility anchor** command.

The Status text box shows one of these values:

UP—The controller is reachable and able to pass data.

CNTRL_PATH_DOWN—The mpings failed. The controller cannot be reached through the control path and is considered failed.

DATA_PATH_DOWN—The epings failed. The controller cannot be reached and is considered failed.

CNTRL_DATA_PATH_DOWN—Both the mpings and epings failed. The controller cannot be reached and is considered failed.

Step 7 See the status of all mobility group members by entering this command:

show mobility summary

Note This command output shows the burned-in MAC address.

Step 8 Troubleshoot mobility issues by entering these commands:

- **debug mobility handoff** {**enable** | **disable**}—Debugs mobility handoff issues.
- **debug mobility keep-alive** {**enable** | **disable**} **all**—Dumps the keepalive packets for all mobility anchors.
- **debug mobility keep-alive** {**enable** | **disable**} *IP_address*—Dumps the keepalive packets for a specific mobility anchor.

Guest Anchor Priority

The guest anchor priority feature provides a mechanism that gives "active/standby" load distribution amongst the anchor controllers. This is achieved by assigning a fixed priority to each anchor controller, by distributing the load to highest priority controller and in round-robin fashion if they have the same priority value.

Releases Prior to 8.1	With Release 8.1
All guest clients are load balanced in round robin fashion amongst anchor controllers	All guest clients are sent to anchor controller with highest priority in relation to local internal controller

Releases Prior to 8.1	With Release 8.1
If an anchor fails, guest clients will be load balanced amongst remaining anchor controllers	If an anchor fails, guest clients will be sent to the next highest priority or round robin if remaining anchors have same priority value

You can configure a priority to the guest anchor when you configure a WLAN. Priority values range from 1 (high) to 3 (low) or primary, secondary or tertiary and defined priority is displayed with guest anchor. Only one priority value is allowed per anchor controller. Selection of guest anchor is round-robin based on a single priority value. If a guest anchor is down, the fallback would be on guest anchors with equal priority. If all guest anchors with same priority value are down, the selection would be on a round-robin basis on next highest priority and so on. Default priority value is 3. If controller is upgraded to Release 8.1, it will be marked with priority 3. Priority configurations are retained across reboots. The priority configuration would be synchronized on HA pair for seamless switchover. Same set of rules apply in determining the anchor controller regardless of IPv4 and/or IPv6 addressing. That is, highest priority value is determinant and not addressing including dual stack case.

Restrictions

- No hard limit on the number of times a priority value is used
- Feature applies only to wireless and "old" mobility model
- Maximum number of supported anchors per WLAN is 24
- Downgrading from Release 8.1 would void this feature since it is not supported on earlier images
- If a guest anchor with higher priority comes up, the existing connections will not shift to the new high priority anchor and only the new connections will go to it
- This feature is applicable when all internal and anchor controllers are using Release 8.1
- There should not be a local address with priority of zero at the Internal/Foreign controller. Priority 0 in the output indicates a local IP address. For example at the anchor controller on DMZ with tunnel termination

Deployment Considerations

- Priority configuration should only be done on foreign controller WLAN. On the mobility list if you are seeing value zero and non-zero that means the same controller is acting as Anchor for few WLANs and foreign controller for few WLAN, if you have controller in DMZ and there is no APs connected to it, then we should not see any non-zero priority for any of its WLANs, as this should be the terminating point for all the clients on the network.
- Ideally we should not see priority zero on foreign controller and non-zero on anchor controller. example: 10.10.10.10(SF) and 20.20.20.20(NY) should not have any priority with zero and DMZ controller 172.10.10.10(SF) and 172.20.20.20(NY) should not have any priority with non-zero values.
- Here priority values zero is not configurable when we select the controller own IP Address as anchor. It will automatically set the priority zero if controller own IP address is selected as anchor.

Examples

- Local anchor controllers may be grouped together with higher priority value than group of remote anchor controllers
- Guest client traffic goes to Anchor controller(s) that is/are local to internal controller rather than remote one(s) due to having higher priority value
- Guest client traffic will be load balanced in round-robin across local anchor controllers since local anchors have same priority value
- If all local anchor controllers fail then traffic will be load balanced in round-robin across remote anchor controller with next priority level

This section contains the following subsections:

Configuring Guest Anchor Priority (GUI)

Procedure

Step 1 Choose **WLANs**.

Step 2 Mouse over the blue down arrow and click **Mobility Anchors**.

Step 3 On the **Mobility Anchors** page, select the mobility anchor from the **Switch IP Address (Anchor)** drop-down list and assign a priority.

Configuring Guest Anchor Priority (CLI)

Procedure

- To configure Guest Anchor priority:
  config wlan mobility anchor add *wlan-id ip-addr* **priority** *prioirity-number*
- To validate proper anchor WLC through assigned client address:
  show client summary ip
- To check whether the expected anchor is getting the request:
  debug mobility handoff enable
- To check the anchor priority list of a WLAN:
  test mobility anchor-prioritylist *wlan-id*

Dynamic Anchoring for Clients with Static IP

At times you may want to configure static IP addresses for wireless clients. When these wireless clients move about in a network, they could try associating with other controllers. If the clients try to associate with a controller that does not support the same subnet as the static IP, the clients fail to connect to the network. You can now enable dynamic tunneling of clients with static IP addresses.

Dynamic anchoring of static IP clients with static IP addresses can be associated with other controllers where the client's subnet is supported by tunneling the traffic to another controller in the same mobility group. This feature enables you to configure your WLAN so that the network is serviced even though the clients use static IP addresses.

How Dynamic Anchoring of Static IP Clients Works

The following sequence of steps occur when a client with a static IP address tries to associate with a controller:

1. When a client associates with a controller, for example, WLC-1, it performs a mobility announcement. If a controller in the mobility group responds (for example WLC-2), the client traffic is tunneled to the controller WLC-2. As a result, the controller WLC 1 becomes the foreign controller and WLC-2 becomes the anchor controller.
2. If none of the controllers responds, the client is treated as a local client and authentication is performed. The IP address for the client is updated either through an orphan packet handling or an ARP request processing. If the IP subnet of the client is not supported in the controller (WLC-1), WLC-1 sends another static IP mobile announce and if a controller (for example WLC-3) that supports the client's subnet responds to that announcement, the client traffic is tunneled to that controller, that is WLC-3. As a result, the controller WLC 1 becomes the export foreign controller and WLC-3 becomes the export anchor controller.
3. Once the acknowledgment is received, the client traffic is tunneled between the anchor and the controller (WLC-1).

Note If you configure WLAN with an interface group and any of the interfaces in the interface group supports the static IP client subnet, the client is assigned to that interface. This situation occurs in local or remote (static IP Anchor) controller.

When AAA override is used along with the interface group that is mapped to WLAN, the source interface that is used for DHCP transactions is the Management interface.

If the interface group that you add to a WLAN has RADIUS Server Overwrite interface enabled and a client requests for authentication, the controller selects the first IP address from the interface group as the RADIUS server.

Note A security level 2 authentication is performed only in the local (static IP foreign) controller, which is also known as the exported foreign controller.

Restrictions on Dynamic Anchoring for Clients With Static IP Addresses

- Do not configure overridden interfaces when you perform AAA for static IP tunneling, this is because traffic can get blocked for the client if the overridden interface does not support the client's subnet. This can be possible in extreme cases where the overriding interface group supports the client's subnet.
- The local controller must be configured with the correct AAA server where this client entry is present.

- The anchor is responsible for sending the accounting packets AVP attribute values input/outputs to the AAA server as it is the point of accounting with the AAA. However, the values sent will be zero. Therefore, only the foreign can send the actual values to the AAA server.

The following restrictions apply when configuring static IP tunneling with other features on the same WLAN:

- Auto anchoring mobility (guest tunneling) cannot be configured for the same WLAN.
- FlexConnect local authentication cannot be configured for the same WLAN.
- The DHCP required option cannot be configured for the same WLAN.
- You cannot configure dynamic anchoring of static IP clients with FlexConnect local switching.
- We recommend that you configure the same NTP/SNTP servers on the Cisco WLCs. If the NTP/SNTP servers are different, ensure that the system time on all Cisco WLCs is the same when NTP/SNTP is enabled. If the system time is not in sync, seamless mobility might fail in some scenarios. Also, a Cisco WLC that has the lagging time with NTP/SNTP enabled drops the mobile announce messages.

Configuring Dynamic Anchoring of Static IP Clients (GUI)

Procedure

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

Step 2 Click the ID number of the WLAN on which you want to enable dynamic anchoring of IP clients. The **WLANs > Edit** page is displayed.

Step 3 Choose the **Advanced** tab to open the **WLANs > Edit (Advanced)** page.

Step 4 Enable dynamic anchoring of static IP clients by checking the **Static IP Tunneling** check box.

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

Configuring Dynamic Anchoring of Static IP Clients (CLI)

config wlan static-ip tunneling {enable | disable} *wlan_id*— Enables or disables the dynamic anchoring of static IP clients on a given WLAN.

To monitor and troubleshoot your controller for clients with static IP, use the following commands:

- **show wlan** *wlan_id*—Enables you to see the status of the static IP clients feature.

```
.............
Static IP client tunneling.............. Enabled
.............
```

- **debug client** *client-mac*
- **debug dot11 mobile** enable
- **debug mobility handoff** enable