Configuring New Mobility

Information About New Mobility

New Mobility enables controllers to be compatible with converged access controllers with Wireless Control Module (WCM) such as the Cisco Catalyst 3850 Series Switches and the Cisco 5760 Series Wireless LAN Controllers. New Mobility provides the ability to run Mobility Controller (MC) functionality on a controller in the Converged Access mode with a Catalyst 3850 mobility agent (MA)

The Mobility Controller is a part of a hierarchical architecture that consists of a Mobility Agent and Mobility Oracle.

A group of Cisco Catalyst 3850 Series Switches' Mobility Agents can form a switch peer group. The internal Mobility Agent of controllers form an independent switch peer group. The Mobility Controller, Mobility Agent, and Mobility Oracle can be in a single controller. Each Mobility Controller forms a subdomain that can have multiple switch peer groups. The controllers are Mobility Agents by default. However, Cisco Catalyst 3850 Series Switch can function both as Mobility Agent and Mobility Controller, or only as a Mobility Agent.

By default, New Mobility is disabled. When you enable or disable new mobility, you must save the configuration and reboot the controller.

Note With Releases 8.4 and 8.5 in a new mobility environment, controllers cannot function as mobility controllers (MC). However, the controllers can function as guest anchors.

New mobility is not supported in Release 8.6 and later releases.

Restrictions for New Mobility

- The keepalives between Mobility Controller and Mobility Oracle are not DTLS encrypted.
- For seamless mobility, the controller should either use new mobility or old mobility (flat mobility).

- Interoperability between two types of mobility is not supported.
- High availability for Mobility Oracle is not supported.
- New Mobility messaging and tunneling are not supported over IPv6. However, New Mobility does support client IPv6 traffic.

Configuring New Mobility (GUI)

Procedure

Step 1 Choose **Controller > Mobility Management > Mobility Configuration** to enable and configure new mobility on the controller.

Note When you enable or disable new mobility, you must save the configuration and reboot the controller.

Step 2 To configure new mobility, select or unselect the **Enable New Mobility (Converged Access)** check box.

Note When you enable new mobility, you must save the configuration and reboot the controller.

Step 3 To configure the controller as Mobility Oracle, select or unselect the **Mobility Oracle** check box.

Note Mobility Oracle is optional; it maintains the client database under one complete mobility domain.

Step 4 To configure multicast mode in a mobility group, select or unselect the **Multicast Mode** check box.

Step 5 In the **Multicast IP Address** text box, enter the multicast IP address of the switch peer group.

Step 6 In the **Mobility Oracle IP Address** text box, enter the IP address of the Mobility Oracle.

You cannot enter a value for this field if you have checked the **Mobility Oracle** check box.

Step 7 In the **Mobility Controller Public IP Address** text box, enter the IP address of the controller, if there is no network address translation (NAT).

Note If the controller has NAT configured, the public IP address will be the network address translated IP address.

Note New mobility does not support IPv6.

Step 8 In the **Mobility Keep Alive Count** text box, enter the number of times a ping request is sent to a peer controller before the peer is considered to be unreachable. The range is from 3 to 20. The default value is 3.

Step 9 In the **Mobility Keep Alive Interval** text box, enter the amount of time, in seconds, between each ping request sent to an peer controller. The range is from 1 to 30 seconds. The default value is 10 seconds.

Step 10 In the **Mobility DSCP** text box, enter the DSCP value that you can set for the mobility controller. The range is from 0 to 63. The default value 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.

Step 11 Click **Apply**.

Step 12 Choose **Controller > Mobility Management > Switch Peer Group** to add or remove members to and from the switch peer group.

This page lists all the switch peer groups and their details, such as bridge domain ID, multicast IP address, and status of the multicast mode. Click the name of the switch peer group to navigate to the **Edit** page and update the parameters, if required.

Step 13 Choose **Controller > Mobility Management > Mobility Controller** to view all the mobility controllers and their details, such as IP address, MAC address, client count, and link status.

Step 14 Choose **Controller > Mobility Management > Mobility Clients** to view all the mobility clients and their parameters.

Step 15 In the **Client MAC Address** and **Client IP Address** text boxes, enter the MAC address and IP address of the mobility client, respectively.

Step 16 In the **Anchor MC IP Address** and **Anchor MC Public IP Address** text boxes, enter the IP address and public IP address of the anchor Mobility Controller, respectively.

Step 17 In the **Foreign MC IP Address** and **Foreign MC Public IP Address** text boxes, enter the IP address and public IP address of the foreign MC, respectively.

Step 18 In the **Client Association Time** text box, enter the time at which the mobility client should be associated with the Mobility Controller.

Step 19 In the **Client Entry Update Timestamp** text box, enter the timestamp at which the client entry should be updated.

Configuring New Mobility (CLI)

Procedure

- Enable or disable new mobility on the controller by entering this command:

  config mobility new-architecture {**enable** | **disable**}

Note When you enable or disable new mobility, you must save the configuration and reboot the controller.

- Enable the Mobility Oracle or configure an external Mobility Oracle by entering this command:

  config mobility oracle {**enable** | **disable** | **ip** *ip_address*}

  Here, *ip_address* is the IP address of the Mobility Oracle. The Mobility Oracle maintains the client database under one complete mobility domain. It consists of a station database, an interface to the Mobility Controller, and an NTP/SNTP server. There can be only one Mobility Oracle in the entire mobility domain.

- Configure the MAC address of the member switch for compatibility between the flat (old) and new mobility by entering this command:

  config mobility group member add *ip_address* {[*group-name*] | *mac-address* | [*public-ip-address*]}

where *ip_address* is the IP address of the member.

group-name is the member switch group name, if it is different from the default group name.

mac-address is the MAC address of the member switch.

Note If the controller has NAT configured, the public IP address will be the network address translated IP address.

Note New mobility does not support IPv6.

- View the details of the mobility controllers according to the Mobility Oracle by entering this command:

  show mobility oracle summary
- View the summary and details of the Mobility Oracle client database by entering this command:

  show mobility oracle client {**summary** | **detail**}
- Verify the mobility statistics by entering this command:

  show mobility statistics
- Verify the mobility configuration by entering this command:

  show mobility summary
- Save your changes by entering this command:

  save config
- Enable or disable debugging of mobility packets by entering this command:

  debug mobility packet {**enable** | **disable**}
- Enable or disable debugging of the Mobility Oracle events and errors by entering this command:

  debug mobility oracle {**events** | **errors**} {**enable**| **disable**}