Monitoring and Validating Mobility

Mobility Ping Tests

Controllers in a mobility list communicate with each other by controlling information over a well-known UDP port and exchanging data traffic through an Ethernet-over-IP (EoIP) tunnel. Because UDP and EoIP are not reliable transport mechanisms, there is no guarantee that a mobility control packet or data packet will be delivered to a mobility peer. Mobility packets may be lost in transit due to a firewall filtering the UDP port or EoIP packets or due to routing issues.

Restrictions for Mobility Ping Tests

- You can test the mobility communication environment by performing mobility ping tests. These tests may be used to validate connectivity between members of a mobility group (including guest controllers). Two ping tests are available:
  - Mobility ping over UDP—This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.
  - Mobility ping over EoIP—This test runs over EoIP. It tests the mobility data traffic over the management interface.
- Only one mobility ping test per controller can be run at a given time.
- These ping tests are not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

Note Any ICMP packet greater than 1280 bytes will always be responded with a packet that is truncated to 1280 bytes. For example, a ping with a packet that is greater than 1280 bytes from a host to the management interface is always responded with a packet that is truncated to 1280 bytes.

- Mobility pings on ports 16666 and 16667 are notable exemptions and these ports cannot be blocked by any ACL.

Running Mobility Ping Tests (CLI)

Procedure

Step 1 To test the mobility UDP control packet communication between two controllers, enter this command:

mping *mobility_peer_IP_address*

The *mobility_peer_IP_address* parameter must be the IP address of a controller that belongs to the mobility list.

Step 2 To test the mobility EoIP data packet communication between two controllers, enter this command:

eping *mobility_peer_IP_address*

The *mobility_peer_IP_address* parameter must be the IP address of a controller that belongs to the mobility list.

Step 3 To troubleshoot your controller for mobility ping, enter these commands:

config logging buffered debugging

show logging

Step 4 To troubleshoot your controller for mobility ping over UDP, enter this command to display the mobility control packet:

debug mobility handoff enable

Note We recommend using an ethereal trace capture when troubleshooting.

WLAN Mobility Security Values

For any anchoring or mobility event, the WLAN security policy values on each controller must match. These values can be validated in the controller debugs. This table lists the WLAN mobility security values and their corresponding security policy.

Table 1: WLAN Mobility Security Values

Security Hexadecimal Value	Security Policy
0x00000000	Security_None
0x00000001	Security_WEP
0x00000002	Security_802_1X
0x00000004	Security_IPSec*
0x00000008	Security_IPSec_Passthrough*
0x00000010	Security_Web

Security Hexadecimal Value	Security Policy
0x00000020	Security_PPTP*
0x00000040	Security_DHCP_Required
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed **Note** Controllers running software release 6.0 or later do not support this security policy.
0x00001000	Security_Web_Passthrough