Overview

Information About Mobility

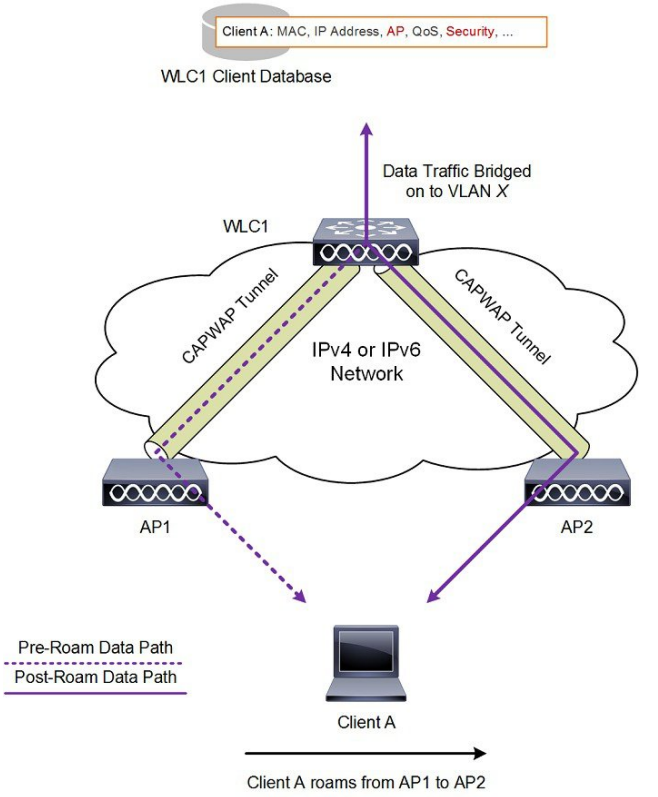
Mobility, or roaming, is a wireless LAN client's ability to maintain its association seamlessly from one access point to another securely and with as little latency as possible. This section explains how mobility works when controllers are included in a wireless network.

When a wireless client associates and authenticates to an access point, the access point's controller places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client.

Note The information about mobility in this section applies to APs in only Local Mode. For APs in FlexConnect mode, see the FlexConnect section.

The figure below shows a wireless client that roams from one local mode access point to another local mode access point when both access points are joined to the same controller.

Figure 1: Intracontroller Roaming

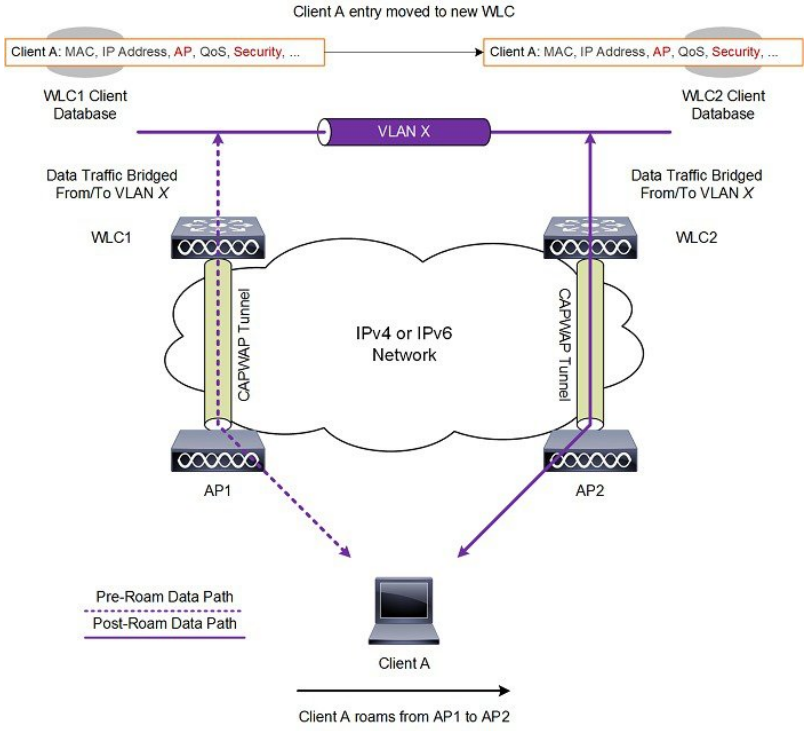


When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well.

The process becomes more complicated, however, when a client roams from an access point joined to one controller to an access point joined to a different controller. It also varies based on whether the controllers are operating on the same subnet.

The figure below shows intercontroller Layer 2 roaming, which occurs when the wireless LAN interfaces of the controllers are on the same IP subnet.

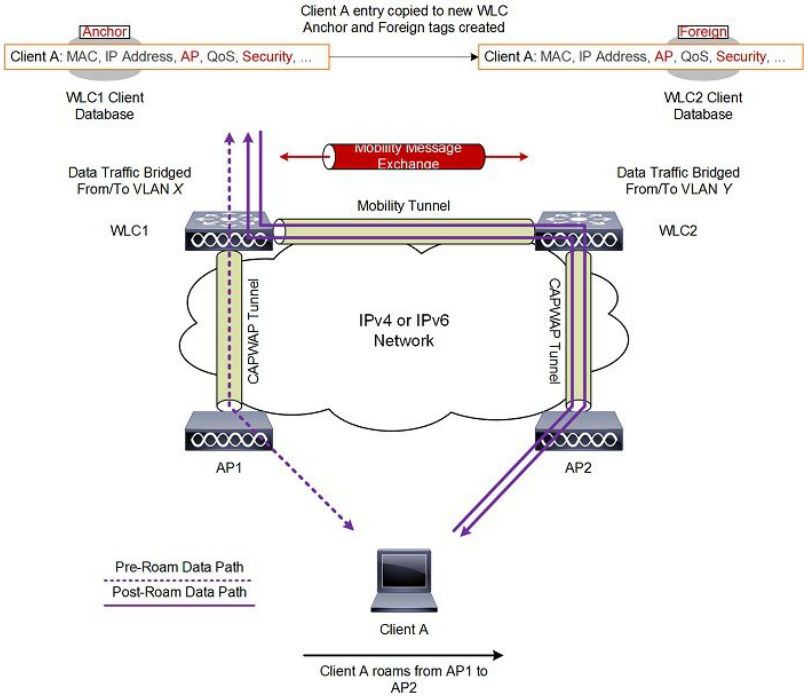
Figure 2: Intercontroller Layer 2 Roaming



When the client associates to an access point joined to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains transparent to the user.

The figure below shows intercontroller Layer 3 roaming, which occurs when the wireless LAN interfaces of the controllers are on different IP subnets.

Figure 3: Intercontroller Layer 3 Roaming



Layer 3 roaming is similar to Layer 2 roaming in that the controllers exchange mobility messages on the client roam. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains transparent to the wireless client, and the client maintains its original IP address.

Guidelines and Restrictions

- If the management VLAN of one controller is present as a dynamic VLAN on another controller, the mobility feature is not supported.
- If a client roams in web authentication state, the client is considered as a new client on another controller instead of considering it as a mobile client.
- When the primary and secondary controller fail to ping each other’s IPv6 addresses, and they are in the same VLAN, you need to disable snooping to get the controller to ping each other successfully.
- Cisco Wireless Controllers (that are mobility peers) must use the same DHCP server to have an updated client mobility move count on intra-VLAN.
- The New Mobility feature is not supported in Release 8.6 and later releases.
- Ensure that the interface name is the same across mobility peers for AAA override to work as expected.
- Up through 8.5, intercontroller roaming was not supported in the following scenarios:
  - Central web authentication (CWA) without 802.1X
  - Web authentication on MAC filter failure

These scenarios are supported with intercontroller roaming beginning with Release 8.6.