Overview of IRCM

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.

Inter-Release Controller Mobility (IRCM) supports seamless mobility and wireless services across different wireless LAN controllers (WLC or also referred to as controllers) that run on different software and controllers (for example, Cisco 8540 Wireless LAN Controller to Cisco Catalyst 9800 Series Wireless Controller) for features such as Layer 2 and Layer 3 roaming and guest access.

While there can be several deployment models that use IRCM within the enterprise, this document specifically covers the IRCM support for interoperability between Catalyst 9800 and Cisco AireOS wireless controllers for the following use cases:

- Customers with existing Cisco AireOS controllers in their networks and adding Catalyst 9800 wireless controllers also known as brownfield deployment.
- Customers with Cisco AireOS controllers deployed as guest anchor and additional Catalyst 9800 wireless controllers added.

- Mobility Concepts, on page 1

Mobility Concepts

As we start to configure mobility, it is important to understand the following concepts.

Key players /Network elements

- Controllers - A Wireless LAN (WLAN) controller manages wireless network access points that allow wireless devices to connect to the network.
- Access points—These devices provide access to the wireless network. Access Points (AP)s are placed in strategic locations to minimize interference.
- Client devices—These include laptops, workstations, IP phones, PDAs, and manufacturing devices that access the WLAN through the access points.

Network settings

VLAN - A logical network to which wireless clients are assigned. It is imperative to declare the VLAN before any configuration can start for roaming or otherwise.

Wireless network parameters

- WLANs and SSIDs - WLAN is a network that allows devices to connect and communicate wirelessly. You can configure WLANs with different Service Set Identifier (SSID)s or with the same SSID. An SSID is the name of the specific wireless network that you want the controller to access.
- Tags & Profiles - On Catalyst 9800 controllers, tags are used to control the features that are available for each Access Point(AP). Tags are assigned to every AP and inside every tag, you can find all the settings that were applied to the AP.
- Policy Tag - On 9800 WLCs, a Policy Tag is the link between a WLAN Profile [Service Set Identifier (SSID)] and a Policy Profile.
  - Policy Profile has details about the Virtual Local Area Network (VLAN) ID, type of traffic -central or local switching, Mobility Anchors, Quality of Service (QoS), timers, and other settings.
  - WLAN Profile has details related to SSID name, WLAN ID, security type for the WLAN, advanced protocols like 802.11k and other settings.

Types of roaming in IRCM

- Intercontroller Roaming Layer 2 - A Layer 2 intercontroller roam occurs when the client traffic is bridged to the same IP subnet (and thus the same VLAN) through the LAN interfaces on both WLCs.
- Intercontroller Roaming Layer 3 - Layer 3 intercontroller roaming occurs when the client associates to an AP on a different WLC and the traffic is bridged to a different subnet.

  In case of roaming between AireOS and Catalyst 9800, it is always a Layer 3 roam, even when both the controllers are on the same VLAN ID.

Mobility Definitions and Controller Roles

- Mobility Groups: A set of controllers in a network can be configured as a mobility group, which allows them to dynamically share important information among them, including the context and state of client devices, and controller loading information.
- Local controller: The controller provides both AP association and IP point of presence, which is where the client enters the wired network
- Anchor controller: The controller provides the IP point of presence only and is always paired with a foreign controller.

  In guest access using guest anchor scenario, anchor refers to one or more controllers deployed in the enterprise DMZ that are used to perform guest mobility tunnel termination, web redirection, and user authentication.
- Foreign controller: The controller provides the AP association only and is always paired with an anchor controller.

  In guest access using guest anchor scenario, foreign refers to the one or more controllers deployed throughout an enterprise campus or at branch location that are used for managing and controlling a group of APs. Foreign controllers map a guest WLAN into a guest mobility tunnel.
- Export Anchor controller: This controller role is relevant in case of a L3 roam for a client, where the controller provides the IP point of presence only and is always paired with an export foreign controller. This is seen with symmetric mobility tunneling and auto-anchoring. Packets for the client are forwarded via a mobility tunnel to the foreign controller for delivery to the client. The anchor controller provides proxy ARP for the client and is the relay to the DHCP server for the client. DHCP packets for the client are forwarded directly to the client via mobility tunnel to the Export Foreign controller.

- Export Foreign controller: This controller role is relevant in case of a L3 roam for a client, when the controller provides the AP association only and is always paired with an export anchor controller. This is seen with symmetric mobility tunneling and auto-anchoring. Packets from the client are forwarded via mobility tunnel to the anchor controller, where they are de-encapsulated and delivered directly to the network. All packets, including ARP and DHCP packets, are sent within the mobility tunnel.
- Auto Anchor: 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 access a guest WLAN throughout an enterprise but still be restricted to a specific subnet.

Types of Tunnel

- Secure - The Catalyst 9800 controllers or the 9800 and AireOS (IRCM image) controllers use Control tunnel 16666 for Mobility Control messages and Data tunnel 16667 for Mobility Data Messages . The control tunnel is always encrypted and data tunnel can be encrypted with DTLS or can be in clear text. This secure link is called Secure Mobility Tunnel.
- EOIP - Controllers (AireOS to AireOS or AireOS (IRCM image) to AireOS (old)) within a mobility group communicate among themselves over a well-known UDP port 16666, and exchange data traffic through an Ethernet-over-IP (EoIP) tunnel. This is an unencrytpted connection.