Seamless Roaming with MR Access Points

As a wireless client roams in an area covered by Meraki APs advertising the same SSID, it will try and associate to the AP that provides the strongest signal. The wireless adapter on the client device measures the RSSI on received frames sent by APs in order to make roaming decisions. A seamless roaming experience is one in which a mobile client can move AP to AP without experiencing a disruption in network aware applications.

When roaming on a mesh network, the mesh will make every effort to keep your existing sessions routed through the gateway Access Point on which the session was initiated. This allows application (Layer 7) sessions to remain connected. Since there is no guarantee that another gateway will have the same backhaul, changing routes over the mesh for a single session is avoided as much as possible. Newer sessions will be initiated via the current best route to the internet.

If an Access Point loses power or otherwise goes down, any active TCP connections will be broken. If there is another AP in range of the client, the client can associate with that AP and reestablish its TCP connection(s). If this AP happens to be a gateway, and other active gateways are present, all associated repeaters will drop connection, scan the environment, and mesh in the most efficient path to the internet.

A Meraki network can be configured to provide seamless roaming for wireless devices if the following guidelines are met:

- The wireless device is associated to an SSID which is set to Bridge mode. Bridge mode provides layer-2 connectivity to the wired LAN. This setting is enabled on an SSID in Dashboard under Configure > Access control.
- All APs in the extended service set must bridge the wireless client to the same IP subnet with the same IP default gateway. If a NAT is used on the upstream firewall, an Internet connection using the same public IP address is also required. This can be verified in Dashboard by adding the Public IP column under Monitor > Access points. The Public IP column must have the same IP address value for all APs.
- Some wireless clients require APs in the extended service set to operate on the same channel. However, if automatic channel selection is enabled to reduce co-channel interference, wireless clients must be capable of roaming between channels and radios on different bands.
- There must not be any gaps in the coverage area between APs. A recommended coverage overlap of 15-20% is recommended. By temporarily setting all APs to the same channel in Dashboard under Configure > Radio settings, it is possible to use the neighbors section on the AP details page to verify an AP is within range of other neighboring APs whose coverage area should overlap. However, the recommended way to determine adequate coverage overlap and AP placement is to perform a pre and post installation site survey. Ekahau makes a commonly used site survey tool to WiFi deployments.

Note: In NAT mode, wireless clients are NAT’d to the IP address of the gateway AP they are associated to. This is called the Meraki NAT. Moving between APs in NAT mode will cause the source IP address of outbound wireless client traffic to change on the outside of the Meraki NAT. Based the nature of NAT mode, connections will break when moving from AP to AP. Applications requiring continuous traffic streams such as VoIP, VPN or media streams will be disrupted when roaming between APs. Traffic such as web browsing which is bursty will break but without a noticeable affect when roaming AP to AP.

Note: Since Bridge mode SSIDs can only allow communication on the same VLAN, L3 Roaming or L3 with a concentrator will be necessary to roam between subnets. Be advised that due to the additional overhead involved with these configurations, they are not ideal for a completely seamless roaming experience.