Roaming Technologies

Wireless deployments that consist of more than one Access Point (AP) broadcasting a wireless network will likely include roaming clients. Since clients can only be associated to one AP at a time, roaming from AP to AP must be quick in order for the user to have a seamless experience. There are a number of technologies that can be employed in order for roaming to be transparent to the end user.

Why does roaming occur?

A wireless client will decide to roam when it detects a better signal from a new AP than the one it is currently associated with. This behavior is normal, especially for mobile devices such as laptops, tablets, and mobile phones.

Challenges with Roaming

When a client roams to a new AP it needs to establish an association/authentication relationship with that AP. In situations where the APs are acting independently of each other, this whole process must occur each time the client moves to a new AP. Without the inclusion of advanced roaming technologies discussed in this article, the client may experience delays when roaming from AP to AP. This results in a service affecting issues like voice drops on VoIP calls and video stuttering on real-time video streams.

Client Tracking

Each AP keeps track of all its connected wireless clients. This includes the client's network access information such as VLAN and group policy (either from Dashboard or RADIUS). During a roam, this information is shared with other APs in the network so the client can maintain their level of access.

Client tracking information is shared with Access Points via broadcast messages, so ensure that port isolation and private VLAN features are not enabled upstream in a configuration that can block broadcasts between APs.

PMKsa caching

PMKsa caching is enabled by default on all Meraki Access Points and is leveraged when using a secure SSID (WPA2-PSK & WPA2-Enterprise). PMKsa caching is also known as "fast roam back" by some vendors. This technology is used when a client device reconnects to an AP it previously had a key exchange with during association. The Session-Timeout value in RADIUS may set a custom session expiration length which would expire the keys after a certain amount of time.

OKC

OKC is enabled by default on all Meraki Access Points and is leveraged when using a secure SSID (WPA2-PSK & WPA2-Enterprise). OKC stands for Opportunistic Key Caching and is a non-standard fast roaming technology supported by Microsoft Windows clients and some Android devices. The Meraki OKC process utilizes key information from the client's first association to generate keys for other APs in the network.
802.11r

802.11r is disabled by default on all Meraki Access Points. 802.11r is a standards-based fast roaming technology, supported by Apple iOS devices and some Android devices, that is leveraged when using a secure SSID (WPA2-PSK & WPA2-Enterprise).

Please refer to our documentation for more information regarding 802.11r.

> While many customers enable 802.11r within their network without issue, some legacy devices may not connect to an 802.11r network. 802.11r is a recommended feature due to its many benefits, however a device audit is encouraged first to ensure that mission critical devices are not affected.

Fast Transition (FT) 802.11r roaming is not supported between Meraki WiFi 6 models and any other MR Access Points (APs) running version 25.x or lower. If you have a mixed deployment with WiFi 6 models and any other model of Meraki APs and 802.11r is either set as enabled or adaptive on any of the SSIDs configuration ensure all your APs are running version 26.4 or higher.

Configuring 802.11r in Dashboard

This feature can be enabled from the Configure > Access control page under Network access > 802.11r. If this option does not appear, a firmware update may be required. 802.11r is also not available while using NAT mode or Layer 3 roaming.

Adaptive 802.11r

Adaptive 802.11r is currently available in MR25.9+ firmware. Please update your firmware to MR25.9 or higher to enable this feature.

Cisco + Apple have co-developed an adaptive roaming technology for iOS devices to improve real-time application experience on enterprise networks. Adaptive 802.11r enables fast roaming for iOS devices detected by the Meraki Access Points while minimizing the possibility of incompatibility issues seen with full 802.11r enabled.

Select "Adaptive" from within the 802.11r dropdown on the Wireless > Access Control page to enable this feature.
802.11e

The 802.11e standard includes a method that allows an AP to advertise its load to wireless clients. Specifically, the QBSS element is used to advertise load via beacons.

Meraki APs will use the QBSS element to report the current channel utilization and the number of stations associated to the wireless access point. Some clients use this information in order to make roaming decisions.

802.11v

802.11v BSS Transition Management (BSS-TM) builds on 802.11k and 802.11e by advertising the client of the best AP to roam to, as determined by load. Meraki APs have 802.11v BSS-TM enabled by default, allowing devices that support the standard to query the AP for a list of recommended APs based on load.

⚠️ Please read our documentation on Client Balancing for more information.