Source: Cisco Meraki – Location Analytics

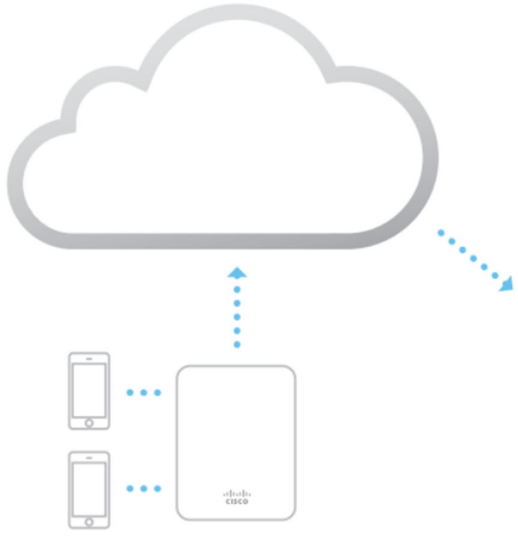
Smartphones with WiFi can now be used as an indicator of customer presence thanks to a WiFi mechanism that is common across all such devices: **probe requests**. These 802.11 management frames are transmitted at regular intervals **from** WiFi devices.

The frames contain information that can be used to identify presence, time spent, and repeat visits within range of any WiFi access point. These devices can be detected by WiFi access points **irrespective** of its WiFi association state meaning that **even if a user does not connect his or her device to the wireless network**, the device's presence can still be detected while the device is within range of the network and the device's WiFi antenna is turned on.

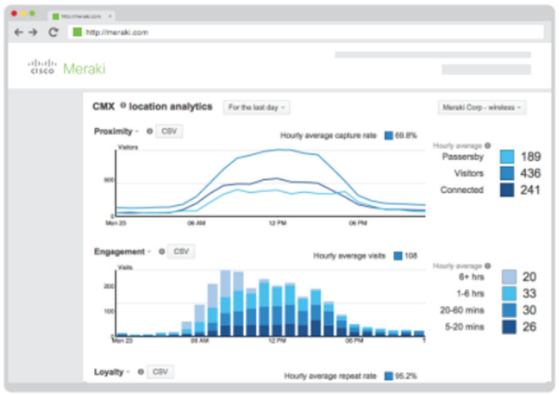
Device State	Probe Request Interval (smartphones)
Asleep (screen off)	~ once a minute
Standby (screen on)	10 - 15 times per minute
Associated	varies, could require user to manually search for networks

Table 1

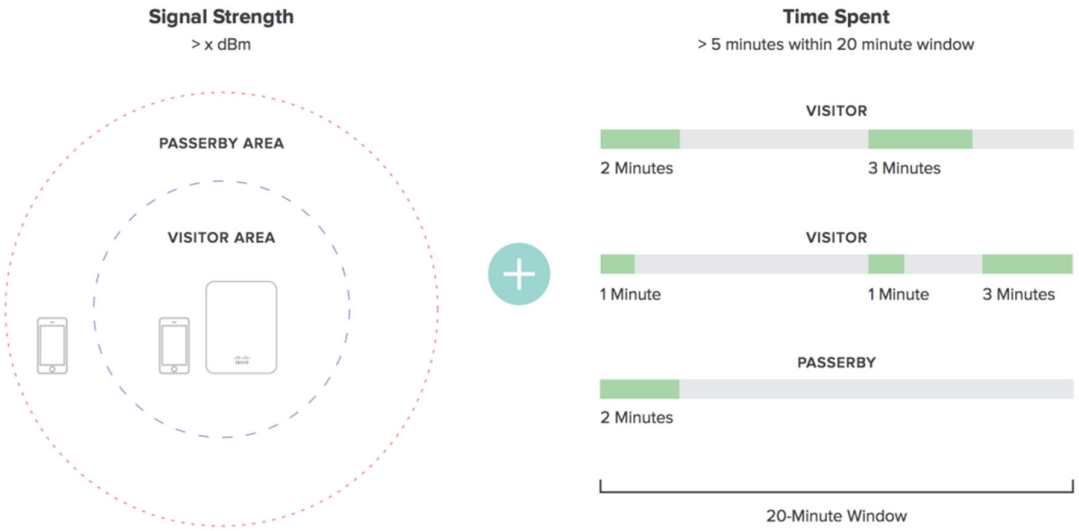
Probe request interval seen on smartphone OS vendors (iOS, Android, others) - varies greatly based on apps, device upgrades, and other factors[4].



Probing and associated clients



Meraki's CMX Location Analytics



Meraki uses probe requests, data frames, and Bluetooth beacon frames to locate and store client location.

Because the location data contain raw MAC addresses, Meraki implemented a number of **security mechanisms to anonymize the data in an irreversible fashion**.

Using a unique Meraki algorithm, the Meraki cloud hashes, salts and truncates MAC addresses so that they are not identifiable. The Meraki cloud then stores only that hashed, salted and truncated version of the MAC address. This anonymization process is described in more detail below.

The hash function is as follows: SHA1 is a widely known one-way cryptographic function. Using SHA1 hashes in this manner is the current industry standard. In order to provide an additional layer of security beyond SHA1 hashing, Meraki's hash function truncates the hash to 4 bytes. This produces an information theoretic loss, as the domain of the function is larger than the range: a 6-byte MAC allows (2^48) possibilities whereas a 4-byte hash allows (2^32) possibilities. This results in 65,000 possible (org + MAC) combinations for each one 4-byte hashed MAC address. Therefore, given a MAC that has been salted, hashed, and truncated with the unique Meraki algorithm, it would be mathematically impossible to know with a reasonable degree of certainty what the original client MAC address was.

The hash function leads to information theoretic loss, and the **original MAC address of client can never be recovered.**

Cisco Meraki includes a customer-specific org-secret in the hash function. As a result, Cisco Meraki does not have any visibility into client behaviour across our customers networks worldwide. And, of course, no Cisco Meraki customer can see the analytics of another customer's organization or where foot traffic goes after leaving the presence of its own WiFi / BLE network.

Finally, Cisco Meraki's website offers a global opt-out feature that allows users to submit the MAC addresses of their devices, after which the Meraki cloud will no longer detect their MAC addresses either for its built-in Location Analytics views or for real-time export via the Scanning API. Cisco Meraki also recommends that retailers and others using the Scanning API post notices on the

availability of this global opt-out in prominent locations, preferably in the storefront or at building entrances where location detection is taking place.