Client Balancing

Overview

Client Balancing uses information about the state of the network and wireless client probes to steer the client to the best available access point during association. Client Balancing is enabled by default on every MR access point. Steering the client to the best available AP improves download and upload performance while reducing loss and latency for mission critical applications. Client Balancing is compatible with all client device types and uses a combination of Meraki-proprietary and industry-standard techniques to gather information and steer clients.

Metrics

A number of metrics are gathered by each access point to ensure that the best client & AP match is made. RF environment metrics and the wireless clients heard by APs are factors in the algorithm. These measurements are captured in real time and shared amongst nearby APs in the Meraki network.

Information exchange

Each AP has a local database that stores metrics of clients both associated and not associated. This information is shared between each AP on the LAN via broadcast messages with an encrypted payload. Note that this message encryption is dynamically configured and secured by the Meraki cloud.
APs on the same LAN segment will automatically send and learn information as described below. This feature was designed for APs in close proximity which typically reside on the same LAN segment (since, for example, a floor or a building may all share a common management VLAN). Since Client Balancing information is sent via broadcasts, any existing network segregation will ensure that Client Balancing intelligence is kept within its relevant area.

Since the feature relies on AP to AP communication, administrators need to ensure that inter-AP communication is allowed and port isolation is turned off.

**Client measurements**

Each AP measures the RSSI for management traffic sent by nearby clients. The Meraki RSSI is a combined measurement of noise floor and client signal strength. Meraki RSSI is also normalized across models of Meraki MR access points. As probes are received and measured, each access point records client measurements in its local database and distributes the info to neighbor access points on the same broadcast domain. As updates are triggered, the tables update in real time allowing the APs to react more quickly when making steering decisions.

**Load measurements**

Each APs current load is also shared with its neighbors. The load metric is defined as the number of current clients connected to the AP. The load metric is used to determine a better possible AP for a client connection.
Distributed intelligence

To achieve the speed required to steer clients, distributed intelligence is required amongst the APs. Client Balancing operates without cloud interaction and utilizes a number of robust features discussed below to make steering decisions:

Per-client AP resource group

The Meraki APs create an AP resource group for each client. A resource group is created based on the notion that not every AP in a network is a good candidate for the client's next connection. When multiple APs hear a given wireless client at 30dB or higher, those APs become a resource group for the client. The load algorithm then attempts to evenly load APs within a client resource group.

If a client is not heard by any AP at an RSSI of 30 or higher, it will not be steered.

Roam-through for VoWiFi/VoIP

Clients that are using real-time applications like VoIP or video collaboration roam from one AP to another using fast roaming technologies. If a Meraki MR access point senses this type of roam by detecting a re-association frame, the client will be permitted to join regardless of whether there is another preferred AP in order to ensure minimal roaming latency for these sensitive applications.

SSID awareness

Client Balancing only analyzes directed probe requests from clients for SSIDs that are configured on the AP when considering an AP in a particular AP resource group. This ensures that Client Balancing will continue to make the most intelligent decisions even if the SSID availability feature is enabled or a radio on a particular AP is disabled.

Sleeping Client Detect times out old data for mobile clients that are not actively roaming but are physically moving. For example, these types of conditions happen when a mobile device is in your pocket while in power save mode. Mobile devices tend to shut down radios in an effort to preserve battery life. When the mobile device leaves sleep mode, it will re-connect to the wireless network.

Many environments are designed with APs in distinct areas where clients in each area are not seen by the APs in other areas. If a client is measured in one area and then moves to a new area while in power save mode, the APs may not be able to track the roam. Measurement data for the client times out after 10 seconds to ensure that APs only within the physical area local to the device are used for steering decisions.

BSSID blacklist protect

For various environmental or wireless adapter driver reasons, a client may not always transition to a preferred AP as offered by the Client Balancing feature. If the client attempts to associate to the same AP a second time, it will always be admitted.

This failsafe mechanism ensures that a client will only experience a brief delay when resending association frames (usually less than 5ms) and that the client does not blacklist the BSSID. BSSID blacklisting is occasionally employed by clients to prevent continuous connection failure.

Steering a client

There are two methods to influence which AP a client connects to next: Association rejections and 802.11v BSS-TM.

Association rejections

During the association process, a client may be rejected with a reason code 17 message indicating that the AP is busy in order to guide the client to a different AP. The problem with this method is that the client is not explicitly instructed as to which access point it should connect.
802.11v basic service set - transition management

Modern clients support 802.11v - BSS-TM (Basic Service Set - Transition Management) which enables network information to be exchanged between the AP and client. During the association process, clients and APs mutually determine if 802.11v BSS-TM can be used. An unsolicited 802.11v BSS-TM frame may be sent from the AP to the client which can indicate to the client that there is a more preferred AP to be connected to. The BSS-TM frame includes a list of neighbors and a report of each of their current loads. This additional information provided to the client reduces client scan times making for graceful steered roams.

Event log reporting

Dashboard will report when Client Balancing is triggered for a client within the Event Log. Using the Event Log’s built-in filtering, an administrator can filter on load balancing events and drill down to a particular access point or client if required. The event will report details about which AP is preferred for the client association.

Legend:

- **load** - Number of current clients on the Client Balancing AP
- **best_ap** - IP address of most preferred AP for client to join
- **best_ap_load** - Number of clients connected to the most preferred AP
- **best_ap_rssi** - Client probe request signal strength measured by preferred AP

<table>
<thead>
<tr>
<th>Time (EST)</th>
<th>Access point</th>
<th>SSID</th>
<th>Client</th>
<th>Event type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 4 19:26:04</td>
<td>BH1 1st Fl Lobby T1</td>
<td></td>
<td>Cole-iPhone</td>
<td>802.11 association rejected for load balancing</td>
<td>load: 10, best_ap: 172.208.154.104, best_ap_load: 0</td>
</tr>
</tbody>
</table>