位置分析

简介

随着移动设备的快速采用，许多组织现在可以利用数据更好地了解实体店环境中的客流量模式和行为。这种位置信息主要基于 802.11 无线和蓝牙标准，可用于吸引用户及优化营销战略。对零售业而言，这类信息有助于抵制在线零售商造成实体店销售量下滑的趋势，因为这些在线零售商多年来一直通过在线工具生成的分析（例如在线广告的点击转化率）掌握着类似数据。

现在，我们可以将具有 WiFi 功能的智能手机作为一种客户光顾指标，这得益于所有此类设备通用的 WiFi 机制：探测请求。这些 802.11 管理帧会定期从 WiFi 设备发送。这些帧中包含可用于识别在线状态、在线时间以及在 WiFi 无线接入点覆盖范围内重复访问次数的信息。无论这些设备的 WiFi 关联状态如何，WiFi 无线接入点都可以检测到它们。也就是说，即使用户的设备并未连接到无线网络，只要设备处于网络范围内且已开启 WiFi 天线，无线接入点仍旧可以检测到设备的在线状态 [1]。

由于智能手机目前在普通人群中的普及率已超过 50%[2]，所以可利用探测请求来构建并检测与给定无线接入点范围内已启用 WiFi 的设备的在线状态有关的重要统计数据集。Meraki 无线接入点和基于云端的 SaaS 网络管理平台基础设施可收集这些数据，汇聚后显示在 Meraki 控制面板中。这个过程是通过直观且可自定义的图表来完成的，商家可以使用这些图表了解捕获率（过客与访客）、用户参与度（所用总时间）和访客忠诚度（新访客与回头客）等趋势。Meraki 能够利用业界领先的基于云端的 SaaS 网络管理平台架构（所有思科 Meraki 产品均已采用）向所有组织提供这些分析。此外，Meraki 扫描 API 能够从观察到的探测请求导出原始数据，而组织可以使用这些原始数据直接与第三方数据仓库或分析平台进行集成。这不仅可以促进与传统客户关系管理 (CRM) 平台进行更深入的集成，而且由于整个过程实时进行，所以还有助于为新一代客户服务计划创造机会。

整体来看，Meraki 的内置位置分析视图和实时位置 API 可以完善现有流量分析功能，帮助全面了解思科 Meraki 网络范围内的设备。本白皮书探讨思科 Meraki 的位置功能，并对这些功能背后的技术及其可以实现的一些使用案例提供相关见解。这些功能是思科 Meraki MR 系列无线接入点的组成部分。

[1] 位置信息的收集和使用已经引起了有关隐私问题的普遍关注。Meraki 对这些问题高度重视，在设计位置分析功能时已充分考虑到隐私问题。用户如果担心此类系统检测到其设备的在线状态，只需关闭设备上的 WiFi 天线即可避免被检测到。

[2] https://www.comscore.com/Insights/Market-Rankings/comScore-Reports-October-2014-US-Smartphone-Subscriber-Market-Share

位置数据收集

思科 Meraki 无线接入点可以通过检测探测请求和 802.11 数据帧，从任意启用 WiFi 的设备上生成在线状态签名，无论该设备是否与网络关联[3]。WiFi 设备通常会根据设备的状态定期发出探测请求（请参阅表 1）。智能手机发送探测请求来发现周围的无线网络，以便用户可以使用这些网络。

设备状态	探测请求间隔（智能手机）
休眠（屏幕关闭）	约每分钟一次
待机（屏幕开启）	每分钟 10 - 15 次
已关联	不尽相同，可能需要用户手动搜索网络

表 1

智能手机操作系统供应商（iOS、Android 等）的探测请求间隔因应用、设备升级和其他因素而存在很大差异[4]。

从所有已连接 WiFi 的设备收到的数据帧以及从一定范围内（通常最远为 100 英尺或更远）发现的所有设备检测到的探测请求，都会在思科 Meraki 无线接入点上生成“发现设备”事件。三频无线接入点有专用的扫描频率，用于全天候侦听所有信道上的探测请求。双频无线接入点缺少扫描频率，可以在 WiFi 设备探测所有信道时侦听到探测请求。已发现的设备信息通过无线接入点与基于云端的 SaaS 网络管理平台之间的安全管理隧道上传。

Meraki 的安全管理隧道已针对发送和接收配置统计信息和大量信息进行了高度优化，而且已发现的设备数据所增加的开销几乎可以忽略不计，管理隧道占用的总带宽仍在 1 千比特/秒左右。

Meraki 无线接入点还能检测到数据帧和探测请求的信号强度，可用于估测 WiFi 设备的实际位置。

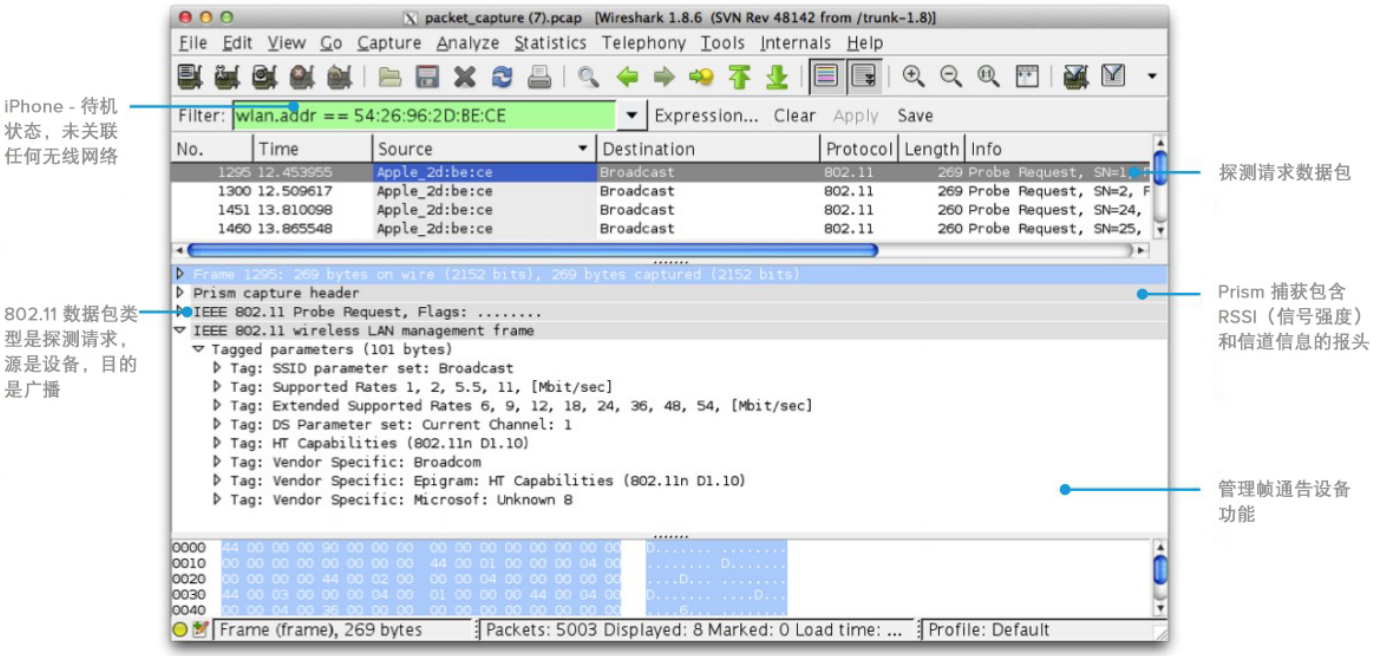


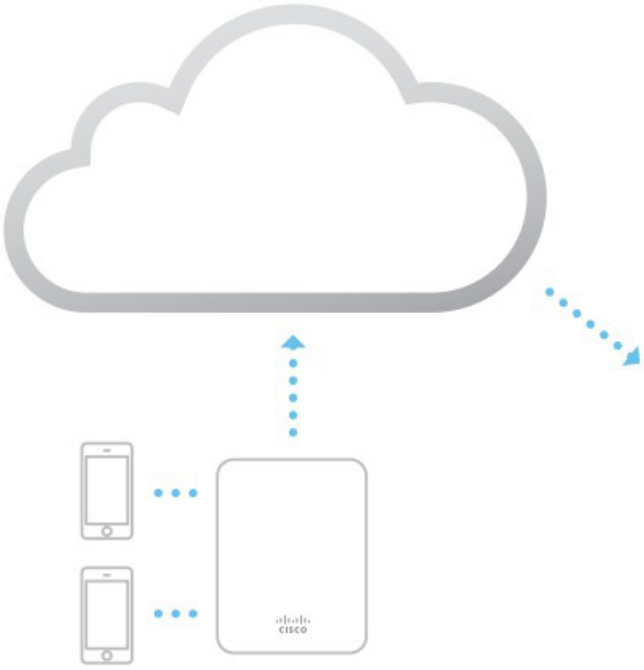
图 1：iOS 设备的典型探测请求 - 从 Meraki 无线接入点捕获的 60 秒数据包捕获（使用 Wireshark 打开）。

[3] 位置数据主要是按设备捕获的，设备的介质访问控制 (MAC) 地址将被用作唯一标识符。作为隐私技术的一部分，有些手机操作系统已添加尝试对设备使用的 WLAN MAC 地址进行随机化处理的功能，使得 Meraki 位置分析等解决方案的跟踪更加困难。随着实施随机化处理的移动设备数量日益增加，用于检测和定位设备的解决方案已发生变化。Meraki 通过 Meraki 扫描 API 提供蓝牙信息等额外功能，让 Meraki 客户能够匿名提供可穿戴式设备的数据，将其包括在位置分析数据集中。

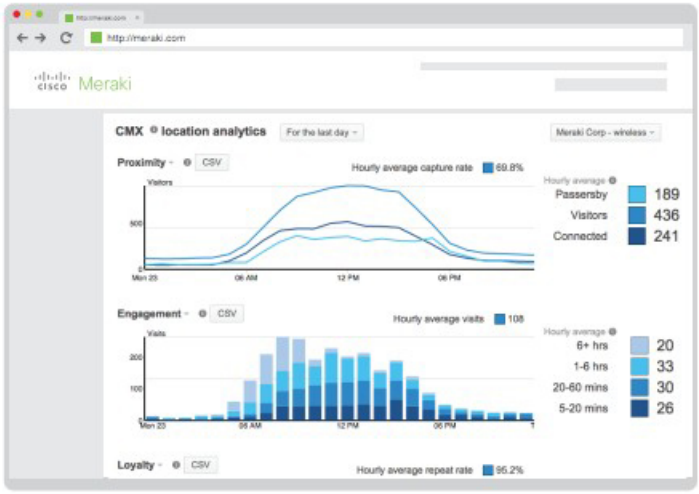
[4] 基于 Meraki 自主实验以及分析合作伙伴实验的实验证据。根据操作系统和手机上安装的应用，此行为往往会有很大差异。例如，如果某个应用非常活跃，则可能导致处于休眠状态的设备每分钟进行多次探测。

数据汇聚和显示

基于云端的 SaaS 网络管理平台收到在线状态签名后，将会汇聚来自同一个网络中所有无线接入点的在线状态签名。汇聚之后，系统会通过一系列计算对从观察到的每个客户端设备收到的数据进行分类，以便稍后显示。例如，零售商需要了解捕获率，即路过店铺的人数与实际进店的人数的比率。基于云端的 SaaS 网络管理平台会分析每个客户端设备的信号强度以及在该位置停留的时间来确定捕获率（如果行人只是快速经过店面，那么信号强度高本身并不能说明有访客）。



探测并已关联的客户端

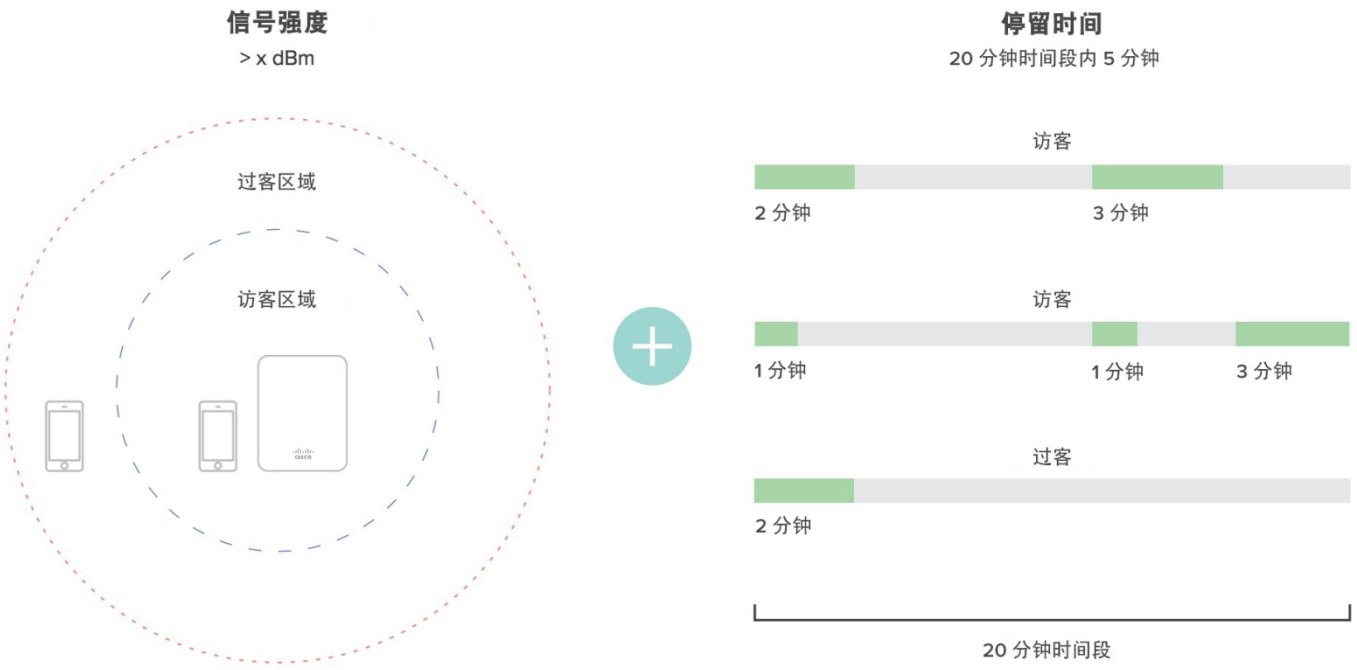


Meraki 的 CMX 位置分析

思科 Meraki 数据库中创建并存储了大量使用各种技术计算出来的不同客户端状态。表 2 显示了类别列表和基础逻辑。

参数	定义	计算
捕获率	变成访客的过客的百分比。过客是指所有已发现的设备，访客则是发现超过一定时间且信号强度高的设备。下图显示的是发现的所有设备，无论他们被视为过客还是访客。访客与发现的客户端总数的比率表示捕获率百分比。	1. 过客分类：任何发现至少一次的设备 2. 访客分类：在 20 分钟时间段内，发现时间超过 5 分钟的设备。接收信号强度指示 (RSSI) 为 15 或更高会打开一个会话，RSSI 为 10 或更高则保持该会话
参与度	该值以分钟为单位，显示访客在无线网络范围内停留的时间。	查看客户端在线状态签名的时间戳，计算一个人在无线网络范围内停留的时间。
忠诚度	新访客与回头客的比例。	每个访客的其他数据库条目检测给定时间段内重复访问的次数。例如，如果一个月内发现某个客户端 4 次，则会将其归类为周访客。8 天内发现至少 5 次的设备会被归类为日访客。

[4] RSSI - 95 = 信号强度（单位：dBm）

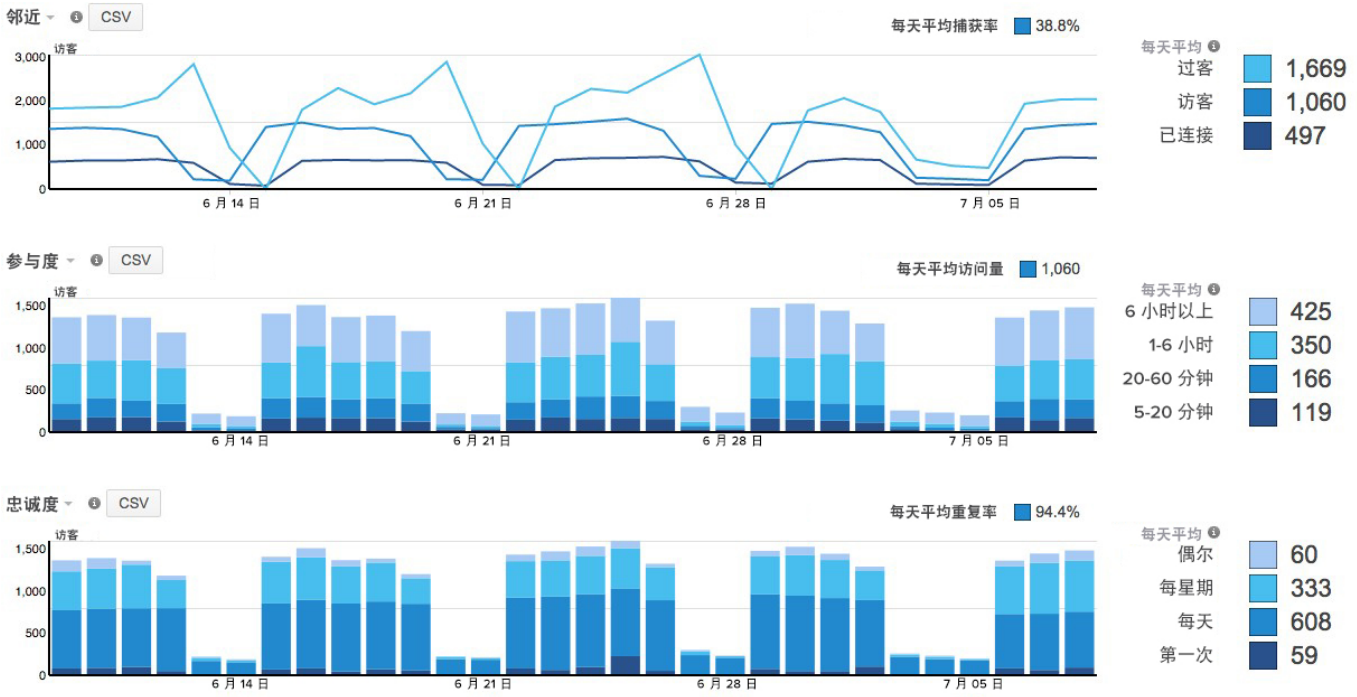


位置分析

当基于云端的 SaaS 网络管理平台实时运行上述计算来计算各种客户端状态时，Meraki 控制面板会通过直观的图表形象地显示捕获率、参与度和忠诚度。这些图表可在简洁和详细两种视图间切换。用户可以通过日历功能放大或缩小给定时间段，查看短至每天的视图（可显示客流量某一天的变化情况和峰值）或长至数月的视图（可显示季节性波动情况）。

通过时间日历功能，您可以选择查看特定时间段；这样，您就可以调整上述图表的 x 轴来查看特定时间段的数据，例如访客数量在特定的某一天或某一周的变化情况。

> **注意**：位置分析数据的保留期为每日分析保留 1 年，每小时分析保留 3 个月。



邻近图

“捕获率”是变成访客的过客的百分比。

“访客”是“访问”您的网络的无线设备。当 Meraki 无线接入点检测到 RSSI 为 15 或更高的探测信号时，即认为发起了一次访问。访客是在 20 分钟时间段内持续发送 RSSI 为 10 或更高的探测信号且时间长达 5 分钟的设备。

“过客”是 Meraki 无线接入点探测到的发送探测信号的设备，但其探测信号和停留时间不符合被视为访客的要求。

邻近图上的访客计数只对其各自的会话计数一次。例如，如果某个设备在中午 12 点被归类为访客，并且其会话保持到下午 8 点，则该设备仅被计为中午 12 点时间段的访客，参与度值为 6 个小时以上。这样，客户就可以确定给定时间有多少访客进店，他们又停留了多长时间。

参与度图

“访客”是保持高信号强度的时间超过 5 分钟的无线设备。该图显示访客在 Wi-Fi 网络范围内停留的时间。

忠诚度图

此图根据访客的回访频率显示访客。例如，周访客表示该访客上个月回访的次数介于 2 次到 6 次之间

运行比较

思科 Meraki 还打造了一款功能强大的比较分析工具，用于帮助洞察给定组织内各个网络之间的关系。通过运行比较，Meraki 控制面板会将第一个数据集的位置数据叠加在第二个数据集上。您可以运行比较来分析不同的数据集，例如：

1. 单个站点在两个不同时间段的情况比较（例如本周与上周）
2. 两个不同的站点或一组站点之间的多站点比较
    - 两个不同站点之间的比较（站点 A 与站点 B）
    - 一个站点与一批站点之间的比较（站点 A 与所有站点，或站点 A 与站点 A 到 D 的平均情况）
    - 两批不同站点之间的比较（所有站点与站点 A 到 D 的平均情况）

展开“分析”页面上显示的时间标尺可以轻松完成两个不同时间段的比较分析。

两批站点之间的比较利用了思科 Meraki 的网络标记功能，管理员可以使用该功能向不同的网络分配一个或多个标记，从而创建分层网络架构。通过这种方式，可以根据所需报告在多站点组织中执行大量比较，例如“为我显示此站点与我组织内的全国平均水平的比较情况”或者“为我显示组织西区站点与东区站点的比较情况”。

由于执行新的位置分析，建议部署思科 Meraki 无线网络的方法保持不变。无需变更无线接入点的放置位置、方向或增加更多无线接入点。前面几个部分介绍的试探方法会自动从现有部署中获取数据，用于分析并提供有关客流量的数据。

在部署已针对位置分析进行优化的思科 Meraki 网络时，应注意若干一般准则和因素，包括：

- 按照常用方法部署无线接入点物理设备，用于提供无线网络覆盖
- 在 Meraki 控制面板中，以每个位置一个网络的组织/网络拓扑来构建部署。由于位置分析数据是以单个网络为基础计算和显示的，所以您可能需要为每个位置创建一个网络（而不是所有位置处于同一个网络中）。控制面板界面经过精心设计，可以方便地管理数百个网络。
- 在“组织”>“概述”页面中标记不同批次的网络。这样，您就可以将一组组站点分组为批次，而且可在比较中根据标记进行数据分析。
- 如果您的网络处于不同的时区，请查看“配置”>“整个网络”设置页面，确保每个网络的时区设置都配置正确，以便能够进行一致的比较。
- 留一些时间（数天）让思科 Meraki 的数据库填充您的网络信息。

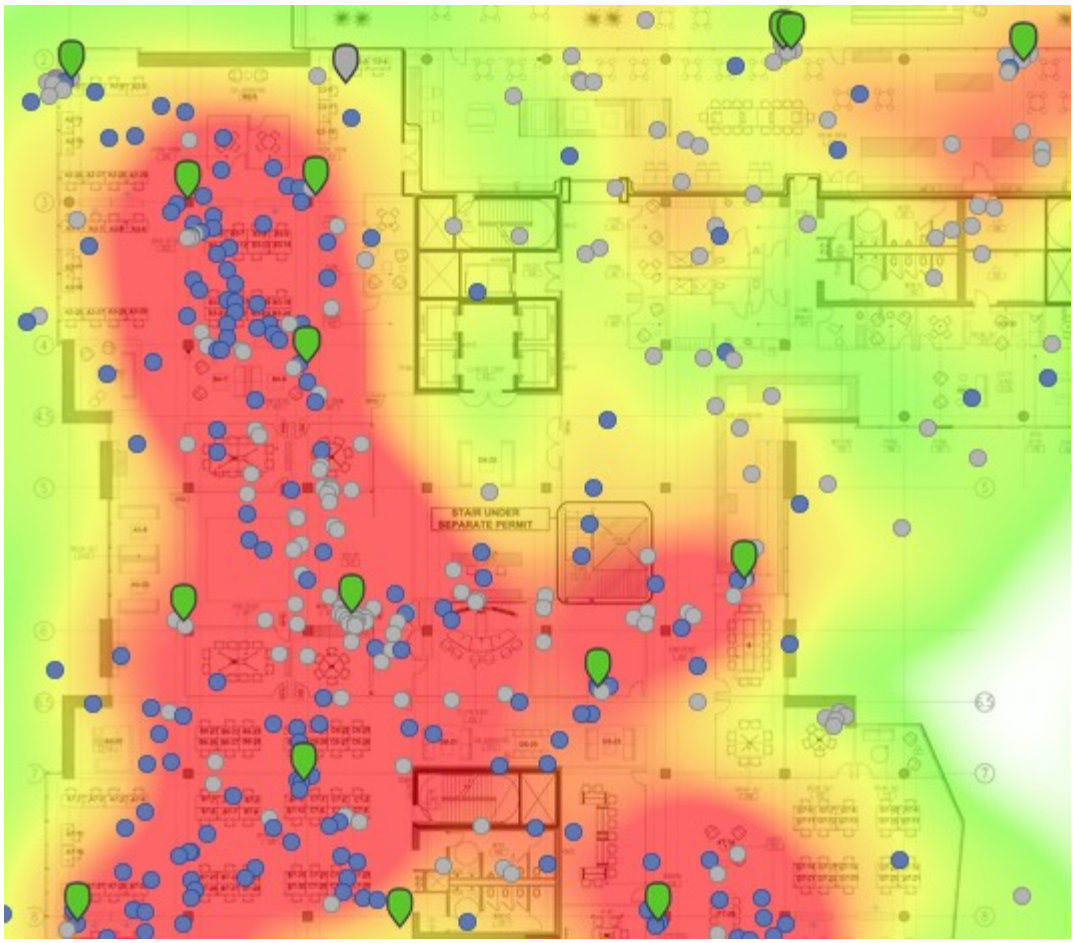
对营销和商业情报团队的价值

所有数据分析和提供的图表背后的目标是为 IT 和非 IT 部门提供一个了解用户光顾情况的平台。通过了解一天内不同时间的客流量和不同站点的捕获率变化情况等模式，IT 部门可以更好地了解网络使用情况和趋势，而非 IT 部门（例如营销和商业情报团队）可以洞察并回答一些问题，例如“根据客流量数据来看，我在站点 A 上的新营销活动是否奏效”或者“我是否需要在高峰时段为站点 B 安排更多员工”。下表突出显示了位置分析可能有帮助的一些不同使用案例。

使用案例
• 检测客户端访问总次数 • 分析并优化窗口转换 • 优化一天内不同时间的人员安排 • 分析访客的停留时间和回访频率 • 在站点之间进行比较或者取一组站点的平均值，以了解低于或高于平均水平的商店客流量、访客停留时间和回访频率 • 优化并运行 A/B 测试，了解一个变量发生变化是否会影响可测量参数（例如捕获率）的结果 • 分析数据并与外部 KPI（例如在每个站点所花的平均时间、每位用户所花的平均时间、每个商店的平均成本）进行比较 • 通过优化策略为每周或季节性波动做好网络准备 • 通过位置分析数据与流量分析和设备指纹数据的关联，可全方位查看用户在线状态、设备及在线行为

位置热图

Meraki 的部分位置功能包括直观显示一天当中人们在特定区域内的哪些具体位置停留的功能（无论他们的设备是否与无线网络关联）。该数据叠加在建筑平面图或 Google 地图上，并可以为网络管理员和营销/运营团队提供有关店铺或建筑内特定区域客流量的信息。



热图页面上的功能

用户可以切换建筑平面图以查看不同楼层的视图，还可以从显示画面中移除无线接入点或显示无线接入点的不同指标（例如型号、当前客户端计数、历史客户端计数等）。热图页面包含“播放”功能，按下“播放”按钮后，可以看到客户端密度在一天中的变化情况。还可以切换日期，查看过去某一天的客户端密度。

基础指标

热图使用两个指标进行计算：(a) 在具体时间段内检测到的设备数量和 (b) 这些设备在区域内停留的时间。地图上的颜色代表“在线”人数最多的区域。强度由特定时间段内检测到的设备数量和这些设备在区域内停留的时间决定。区域颜色可能是暗红色，表示检测到了很多设备或有一些设备在一个小时内一直停留在该区域内。

客户端指标

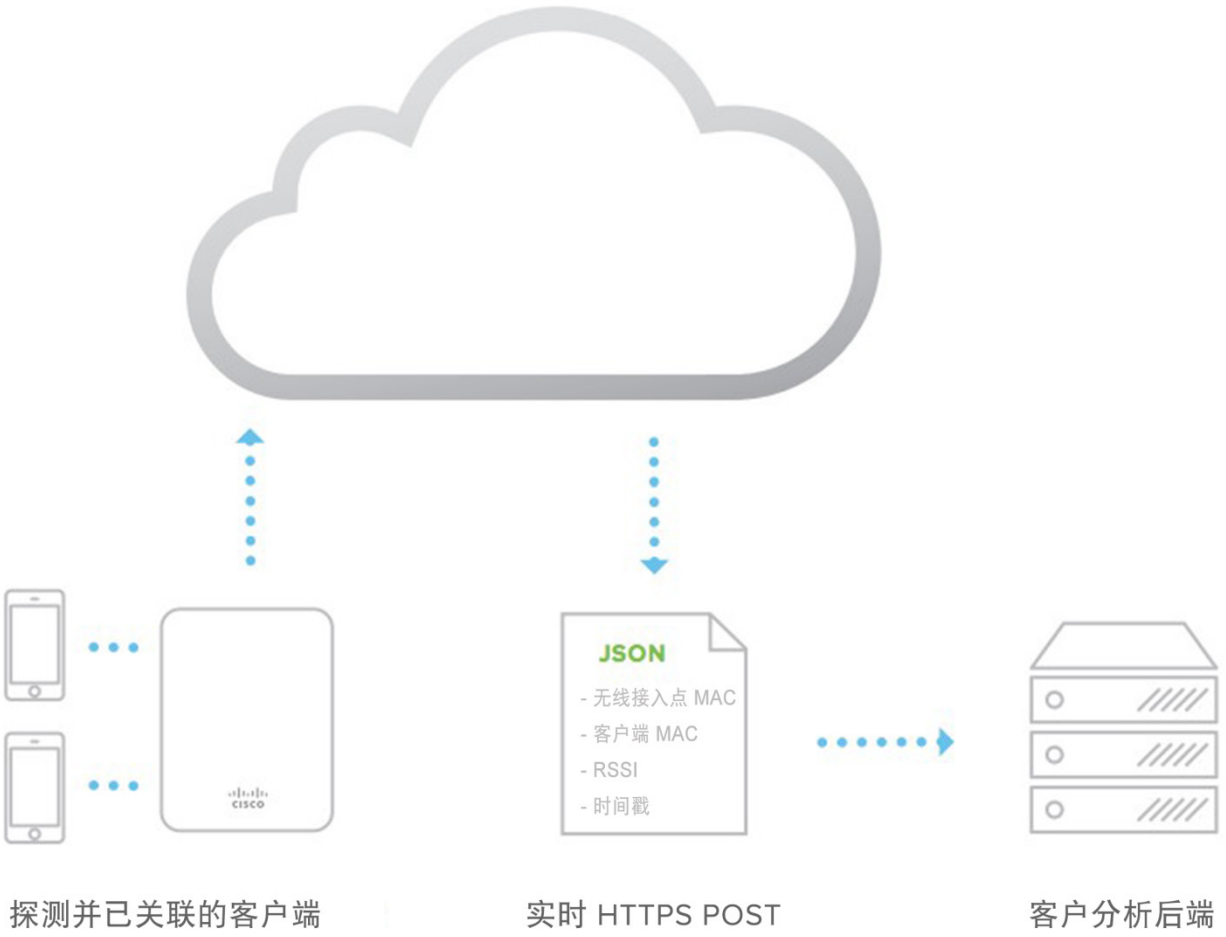
热图上还将绘制通过计算得出的客户端在无线网络中的位置。灰色圆圈代表仅探测但未与无线网络关联的客户端。蓝色圆圈代表已连接到其中一个由无线网络提供服务的 SSID 的客户端。

扫描 API

简介

得益于配备 WiFi 和 BLE 的智能设备得到广泛使用，思科 Meraki 无线接入点可以检测并提供位置分析，以便报告用户的客流量行为。这在多站点零售或企业部署中特别有用，因为在这些部署中，管理员或 IT 部门以外的其他部门希望了解有关趋势和用户参与度的详细信息。思科 Meraki 与 WiFi 网络中有关客户端设备、应用和网站的传统报告功能相结合，可以让您全面了解在线和离线用户流量。

利用我们分布于世界各地的数据中心架构，思科 Meraki 已构建可汇聚来自数千个终端的数据的端到端系统，以便有效地收集、分析并在 Meraki 控制面板中显示这些数据。用户可以在不同站点和时间段之间进行比较，而且思科 Meraki 的网络标记功能支持根据区域、地域或任何其他偏好将网络组合到一起，从而创建不同批次的网络，因此这种比较的变化形式完全不受限制。除了内置的位置分析视图外，思科 Meraki 客户还能通过扫描 API 检测并汇聚实时数据，用于自定义应用。



扫描 API 实时从基于云端的 SaaS 网络管理平台提供数据，并可用于实时检测 WiFi（关联和非关联）和低功耗蓝牙 (BLE) 设备。通过 JSON 数据的 HTTP POST 请求将元素导出到指定的目的服务器。网络中所有无线接入点的原始数据在基于云端的 SaaS 网络管理平台中汇聚，并直接从基于云端的 SaaS 网络管理平台发送到组织的数据仓库或商业情报中心。JSON POST 请求发送频繁，通常每分钟为每个无线接入点发送一批。

基于云端的 SaaS 网络管理平台使用控制面板上“地图和建筑平面图”中的无线接入点物理位置来估测客户端的位置。地理位置坐标（纬度、经度）和 X、Y 位置数据的准确性可能因许多因素而有所不同，应当视作尽力而为的估测值。无线接入点位置、环境条件和客户端设备方向都可能影响 X、Y 估测值。调整无线接入点位置或添加额外的无线接入点有助于提高结果的准确性。因此，过滤数据点以选择最小 RSSI 值、最大不确定性值或 API 中包含的其他数据元素是很常见的做法。

扫描数据元素

扫描 API 版本 2.0 数据架构的设备分类和位置信息。基于云端的 SaaS 网络管理平台使用控制面板上“地图和建筑平面图”中的无线接入点物理位置来估测客户端的位置。

数据元素

名称	格式	说明
apMac	字符串	观察的无线接入点的 MAC 地址
apTags	[字符串]	应用到控制面板中无线接入点的所有标记的 JSON 数组
apFloors	[字符串]	显示此无线接入点的所有建筑平面图名称的 JSON 数组
clientMac	字符串	设备 MAC
ipv4	字符串	“主机名/地址”格式的客户端 IPv4 地址和主机名；
ipv6	字符串	“主机名/地址”格式的客户端 IPv6 地址和主机名；若无主机名，则仅使用“/地址”，若无法提供则为 null 值
seenTime	ISO 8601 日期字符串	观察时间（协调世界时）；示例：“1970-01-01T00:00:00Z”
seenEpochinteger		观察时间（自 UNIX 时期以来的秒数）
ssid	字符串	客户端 SSID 名称；若设备未连接则为 null 值
rssi	整数	无线接入点发现的设备 RSSI
Manufacturestrring		设备制造商；若无法确定制造商则为 null 值
os	字符串	设备操作系统；若无法确定操作系统则为 null 值
location	位置	设备的地理位置；若无法确定位置则为 null 值
lat	十进制数	设备的赤道北纬度数
lng	十进制数	设备的本初子午线西经度数
unc	十进制数	以米为单位的不确定性值
x	[十进制数]	相对于每个建筑平面图左下角的 x 偏移量（单位：米）的 JSON 数组
y	[十进制数]	相对于每个建筑平面图左下角的 y 偏移量（单位：米）的 JSON 数组

HTTP POST 正文格式

```
{
  "version":"2.0",
  "secret":<string>,
  "type":<event type>,
```

```
  "data":<event-specific data>
}
```

事件特定数据格式

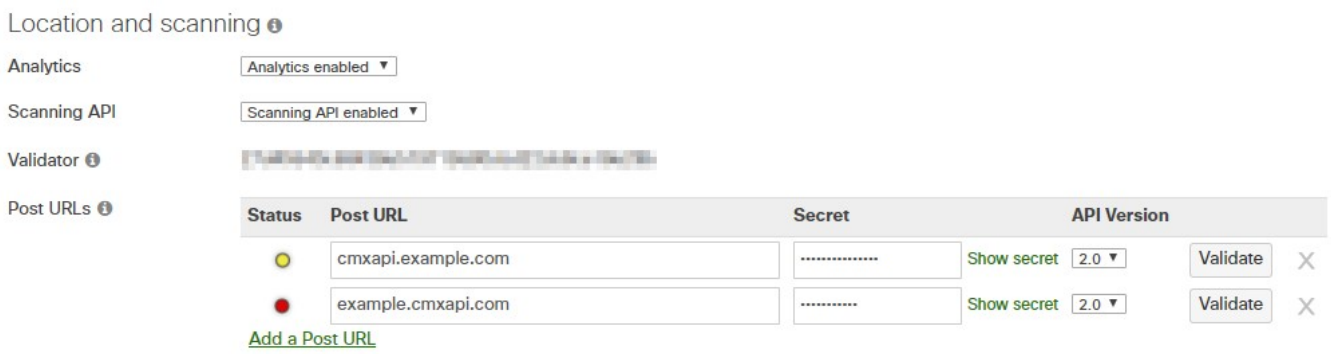
```
{
 "apMac"：<string>,
 "apTags"：[<string, ...],
 ors"：[<string>, ...],
 "observations"：[
  {
   "clientMac"：<string>,
   "ipv4"：<string>,
   "ipv6"：<string>,
   "seenTime"：<string>,
   "seenEpoch"：<integer>,
   "ssid"：<string>,
   "rssi"：<integer>,
   "manufacturer"：<string>,
   "os"：<string>,
   "location"：{
    "lat"：<decimal>,
    "lng"：<decimal>,
    "unc"：<decimal>,
    "x"：[<decimal>, ...],
    "y"：[<decimal>, ...]
   },
  },...
 ]
}
```

启用扫描 API

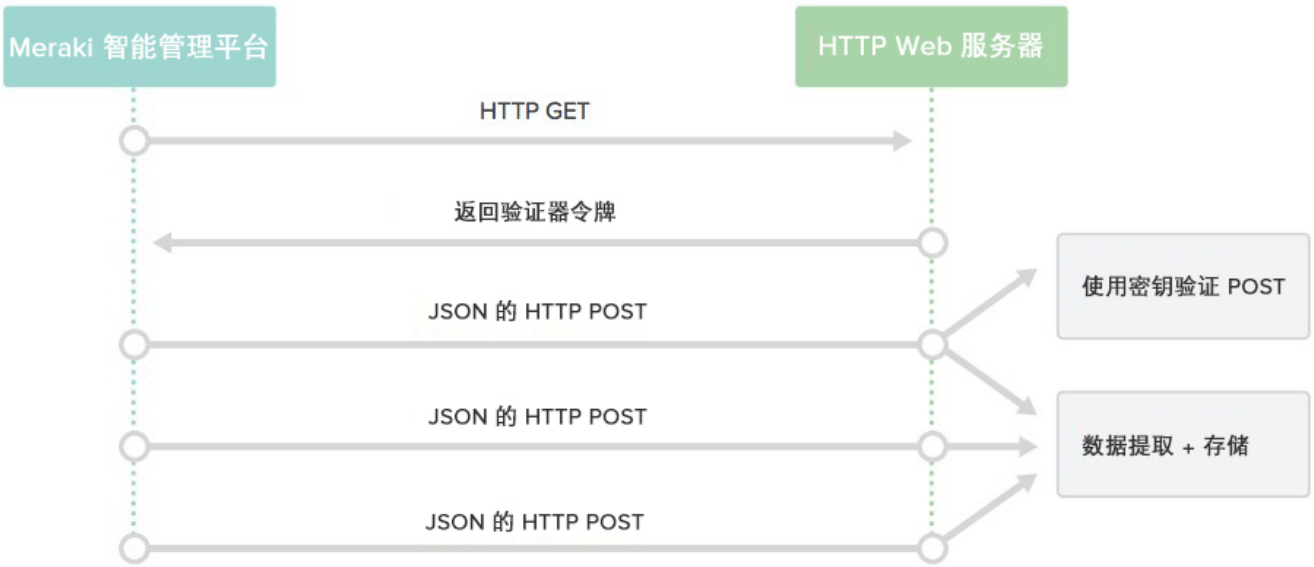
在 Meraki 控制面板的**整个网络 > 常规**设置页面中，只需几个简单的步骤即可完成扫描 API 配置：

1. 配置并托管您的 HTTP 服务器以接收 JSON 对象。
   - 版本 1 接收器示例
   - 版本 2 接收器示例 (https://github.com/meraki/cmx-api-app)
2. 从下拉列表框中选择已启用的扫描 API 以开启 API。
3. 指定 POST URL 和身份验证密钥（密钥由 HTTP 服务器用于验证 JSON POST 请求是否来自基于云端的 SaaS 网络管理平台）
4. 指定 HTTP 服务器准备接收和处理的扫描 API 版本。

5. 点击**验证**按钮，然后在验证成功后点击**保存**按钮保存页面。
6. 在第一次连接时，基于云端的 SaaS 网络管理平台会执行一个 HTTP GET 请求；该服务器必须返回特定组织的验证器字符串作为响应，以确认该组织的身份为思科 Meraki 客户。然后，基于云端的 SaaS 网络管理平台将开始执行 JSON POST。



基于云端的 SaaS 网络管理平台与第三方服务器之间的协议流：



蓝牙扫描 API

具有集成的低功耗蓝牙 (BLE) 频率的 Meraki 无线接入点可以检测并定位附近的低功耗蓝牙设备。然后，通过 API 向第三方应用提供此数据。此类设备的示例包括智能手表、基于电池的信标、Apple iBeacons、健康监测器和远程传感器。

启用蓝牙扫描

基于云端的 SaaS 网络管理平台使用控制面板上“地图和建筑平面图”中的无线接入点物理位置来估测客户端的位置。地理位置坐标（纬度、经度）和 X、Y 位置数据的准确性可能因许多因素而有所不同，应当视作尽力而为的估测值。无线接入点位置、环境条件和客户端设备方向都可能影响 X、Y 估测值；实验有助于提高结果的准确性或确定对数据点而言可以接受的最大不确定性值。

要实现 BLE 设备定位，请在无线接入点上启用 BLE 扫描频率。如下面的图 3 所示，在**无线** > **蓝牙设置** > **扫描**设置页面的“扫描”部分，选择“开”即可启用 BLE 扫描：

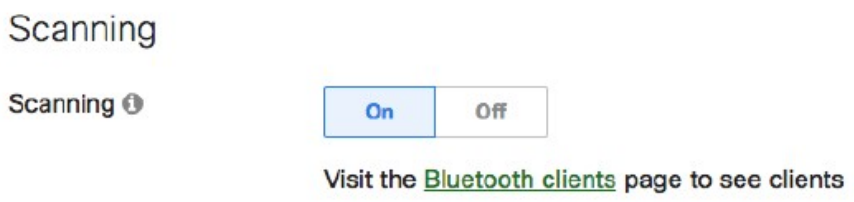


图 3：启用 BLE 扫描 BLE 扫描 API

蓝牙 API 数据元素

名称	格式	说明
apMac	字符串	观察的无线接入点的 MAC 地址
apTags	[字符串]	应用到控制面板中无线接入点的所有标记的 JSON 数组
apFloors	[字符串]	显示此无线接入点的所有建筑平面图名称的 JSON 数组
clientMac	字符串	设备 MAC
seenTime	ISO 8601 日期字符串	观察时间（协调世界时）；示例：“1970-01-01T00:00:00Z”
seenEpochinteger		观察时间（自 UNIX 时期以来的秒数）
rssi	整数	无线接入点发现的设备 RSSI
location	位置	设备的地理位置；若无法确定位置则为 null 值

名称	格式	说明
lat	十进制数	设备的赤道北纬度数
lng	十进制数	设备的本初子午线西经度数
unc	十进制数	以米为单位的不确定性值
x	[十进制数]	相对于每个建筑平面图左下角的 x 偏移量（单位：米）的 JSON 数组
是	[十进制数]	相对于每个建筑平面图左下角的 y 偏移量（单位：米）的 JSON 数组

启用具有 BLE 扫描功能的扫描 API，数据将在单一数据源中同时包括无线接入点发现的 WiFi 和蓝牙设备。事件类型 **BluetoothDevicesSeen** 用于标识蓝牙频率的观察结果。以下是扫描 API 用于蓝牙设备的 JSON 格式。

HTTP POST 正文格式

```
{
  "version":"2.0",
  "secret":<string>,
  "type":"BluetoothDevicesSeen",
  "data":<event-specific data>
}
```

位置和隐私

Meraki 深知，有些最终用户可能会对位置信息的收集和使用存在担忧。为了解决这些问题，Meraki 在开发定位服务时便已考虑到隐私问题，纳入了大量安全机制来消除其收集的数据中的唯一可识别元素。Meraki 也建议客户和合作伙伴实施多种保护隐私的功能。

Meraki 使用探测请求、数据帧和蓝牙信标帧来定位和存储客户端位置。因为位置数据包含原始 MAC 地址，Meraki 实施了大量的安全机制，以不可逆的方式对数据进行匿名处理。基于云端的 SaaS 网络管理平台使用一种独有的 Meraki 算法，对 MAC 地址进行散列计算、加盐并截断，使其无法识别。然后，基于云端的 SaaS 网络管理平台只存储进行散列计算、加盐并截断后的 MAC 地址版本。下面对此匿名化过程进行了更加详细的介绍。

散列函数如下：

hash(mac bytes, org secret) =

SHA1(mac bytes ++ org secret).takeRight(4)

其中：

++ 表示串联；

takeRight(4) 返回 SHA1 的 4 个最低有效字节；

org secret 是每个客户的盐值。

示例：

客户端 MAC 为 11:22:33:44:55:66

org secret 为 t3lrdd

SHA1 (112233445566t3lrdd) 的 4 个最低有效字节 = 0x0e456406

SHA1 是一种众所周知的单向加密函数。以这种方式使用 SHA1 散列值是目前的行业标准。为了在 SHA1 散列之外再增加一层安全防护，Meraki 的散列函数还将散列值截断为 4 个字节。理论上这会造成信息丢失，因为函数的域大于这个范围：6 字节 MAC 有 (2 ^48) 种可能性，而 4 字节散列值只有 (2 ^32) 种可能性。这会导致经过散列计算的每一个 4 字节 MAC 地址有 65,000 种可能的 (org + MAC) 组合。因此，鉴于已经使用独有的 Meraki 算法对 MAC 进行加盐、散列计算和截断处理，用数学方法是不可能有一定把握地知道原始客户端 MAC 地址是什么的。

散列函数导致理论上的信息丢失，使客户端的原始 MAC 地址永远也无法恢复。

思科 Meraki 在散列函数中包含一个客户特定的 org-secret。因此，思科 Meraki 根本无法看到客户网络范围内的任何客户端行为。当然，也没有任何思科 Meraki 客户可以看到其他客户组织的分析或者客流离开他们自己的 WiFi/BLE 网络后的去向。

最后，思科 Meraki 网站还提供全局退订功能，用户可以通过该功能提交其设备的 MAC 地址，此后基于云端的 SaaS 网络管理平台将不再检测其 MAC 地址用于内置的位置分析视图或通过扫描 API 实时导出。思科 Meraki 还建议使用扫描 API 的零售商和其他人，在醒目的位置（最好是在店面或建筑物入口等进行位置检测的地方）张贴有关提供此全局退订功能的通知。

数据隐私

前文介绍的思科 Meraki 扫描 API 将原始 MAC 地址导出到指定的第三方服务器。我们实施了大量的隐私保护机制，其中包括：

不关联客户身份机制

思科 Meraki 不会直接提供任何将 MAC 地址与客户身份相关联的方法。这些系统必须由客户、合作伙伴或运营商独立构建和托管。

不与客户联系机制

思科 Meraki 不提供任何可供他人以任何方式使用 API 数据与客户联系的机制。如需与用户实时互动，思科 Meraki 客户必须自行构建并维护用于联系客户的平台。

最佳做法建议

思科 Meraki 对其 API 用户提出了许多最佳做法建议，其中包括：

- 选择使用 API 的思科 Meraki 客户应在进行身份关联时清楚地说明（例如，通过启动页面或通过手机应用），可能会将用户提供的信息与设备的 MAC 地址相关联以促进更全面的参与。
- 现场通知：与使用内置位置分析一样，应在使用位置 API 数据的区域将通知张贴在显眼的位置。
- 退订：除了提供退订政策外，思科 Meraki 客户还应让自己的客户知道思科 Meraki 的全局退订政策（允许通过 MAC 地址退订），并提供访问思科 Meraki 退订页面的直观方法。思科 Meraki 的全局退订页面位于：https://account.meraki.com/optout。

故障排除

思科 Meraki 扫描 API 是功能强大的资源。例如，位置 API 与建筑平面图同步结合使用，可在设备经过特定的建筑平面图时报告客户端位置。

在本文中，“终端”指接收扫描 API POST 请求的服务器。根据配置，除了铁路服务等后端应用外，这可能还包括 Apache 或 Nginx 等 Web 引擎。

收不到扫描 API 数据

收不到扫描 API 数据的问题可以分为两种类型。终端要么能看到来自控制面板的传入 TCP 连接，要么看不到：

没有来自控制面板的连接

如果终端看不到来自控制面板的通信，第一步需要确保终端与控制面板之间存在基本的网络连接。调查终端上游存在的任何防火墙的日志，确保没有执行过滤。如果不存在防火墙或防火墙相对宽松，您应该能够从任意外部地址通过 Telnet 连接到终端。

如果终端响应慢，也可能会在短时间内（15 至 20 分钟）缺少数据，如下所述。如果终端日志未指出响应时间长和出错，可从其他来源确认与终端的连接，并且未执行流量过滤，则请联系思科 Meraki 支持部门寻求进一步帮助。

有来自控制面板的连接

如果能看到来自控制面板的 TCP 连接但收不到扫描 API 数据，可以考虑以下可能的原因：

- **HTTPS 的注意事项**

使用 HTTPS 时，终端必须有一个由有效的公共证书颁发机构 (CA) 签名的有效证书。如果证书并非由公认 CA 签名、已过期、已吊销或因其他原因而无效，则无法建立会话以允许传入 POST。

在某些情况下，如果由控制面板未知的中间 CA 签名，则签名证书可能虽有效但仍无法识别。因此，我们建议在使用 HTTPS 时包括完整的 CA 链。

- **终端响应时间太长**

如果终端响应 POST 请求所用的时间特别长（500 毫秒或更长时间），该终端的信息将被丢弃而不发送。建议应用对传入扫描 API 数据与出于此原因路由的数据分开处理。

- **终端返回错误**

检查应用和服务日志，确保终端应用未报告错误。请向您的终端应用/服务供应商索取文档并寻求有关故障排除的帮助。

- **URL 无法验证**

URL 验证期间，终端必须返回正文仅包含验证器字符串的 200 OK 响应。如果响应不是 200 OK，或正文与验证器字符串并不完全匹配，验证将失败，而且无法将终端 URI 保存为条目。使用 Google Chrome 或 Firefox 等浏览器直接访问 POST URL 或使用 curl 生成 GET 请求是检查终端是否响应正确的方法。

数据格式错误

当且仅当客户端与网络关联时，才会包含一些特定信息。这其中包括制造商、操作系统、SSID 和 IP 地址。某些信息（例如位置值或无线接入点标记）仅当可用时才会包括在内。其他信息应始终包括在内并始终有一个值。如果没有，请联系 Meraki 支持部门。

其他资源

有关思科 Meraki 的位置分析和 API 的详细信息，请参阅以下资源：

- 位置分析
- 位置 API 概述