演示9800无线局域网控制器上的客户端分析

目录

简介

本文档介绍设备分类和分析如何在Cisco Catalyst 9800无线LAN控制器上运行。

使用的组件

- 运行17.2.1映像的9800 CL WLC
- 1815i接入点
- Windows 10 Pro无线客户端
- 思科ISE 2.7

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

分析过程

本文深入了解设备分类和分析如何在Cisco Catalyst 9800无线LAN控制器上运行，描述了潜在的使用案例、配置示例以及排除故障所需的步骤。

设备分析是一项功能，用于查找有关已加入无线基础设施的无线客户端的其他信息。

执行设备分析后，可以使用它来应用不同的本地策略或匹配特定RADIUS服务器规则。

Cisco 9800 WLC能够执行三(3)种类型的设备分析：

1. MAC地址OUI
2. DHCP
3. HTTP

MAC地址OUI分析

MAC地址是每个无线（有线）网络接口的唯一标识符。它是通常以十六进制格式MM:MM:MM:SS:SS:SS写下的48位数字。

前24位（或3个二进制八位数）称为OUI（组织唯一标识符），它们唯一标识供应商或制造商。

它们由IEEE购买和分配。一家供应商或制造商可以购买多个OUI。

示例：

```
00:0D:4B - owned by Roku, LLC
90:78:B2 - owned by Xiaomi Communications Co Ltd
```

无线客户端与接入点关联后，WLC会执行OUI查找以确定制造商。

在Flexconnect本地交换部署中，AP仍会将相关客户端信息中继到WLC（例如DHCP数据包和客户端MAC地址）。

仅基于OUI的分析极其有限，可以将设备分类为特定品牌，但它无法区分笔记本电脑和智能手机。

本地管理的MAC地址问题

出于隐私考虑，许多制造商开始在他们的设备中实施mac随机化功能。

本地管理的MAC地址是随机生成的，并且地址第一个八位组的第二个最低有效位设置为1。

此位充当一个标志，用于宣布mac地址实际上是一个随机生成的地址。

本地管理的MAC地址有四种可能的格式（x可以是任何十六进制值）：

```
x2-xx-xx-xx-xx-xx
x6-xx-xx-xx-xx-xx
xA-xx-xx-xx-xx-xx
xE-xx-xx-xx-xx-xx
```

默认情况下，Android 10设备在每次连接到新的SSID网络时使用随机生成的本地管理MAC地址。

由于控制器识别出地址是随机化的，并且不执行任何查找，因此此功能完全破坏了基于OUI的设备分类。

DHCP分析

DHCP分析由WLC通过调查无线客户端发出的DHCP数据包来执行。

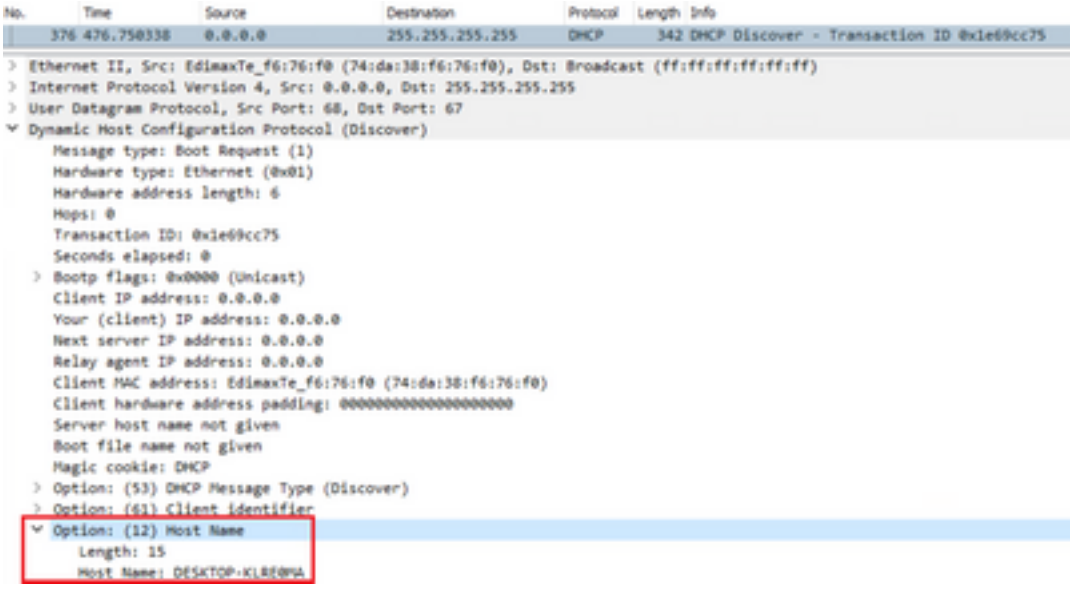
如果使用DHCP分析对设备进行分类，**show wireless client mac-address [MAC_ADDR] detailed**命令的输出包括：

```
Device Type       : Microsoft-Workstation
Device Name       : MSFT 5.0
Protocol Map      : 0x000009  (OUI, DHCP)
Protocol          : DHCP
```

WLC检查无线客户端发送的数据包中的多个DHCP选项字段：

1.选项12 — 主机名

此选项表示客户端主机名，可在DHCP发现和DHCP请求数据包中找到：



2.选项60 — 供应商类别标识符

此选项也在DHCP发现数据包和请求数据包中找到。

使用此选项，客户端可以向DHCP服务器标识自身，然后可以将服务器配置为仅响应具有特定供应商类别标识符的客户端。

此选项最常用于识别网络中的接入点，并且仅使用选项43对接入点做出响应。

供应商类标识符示例

- **"MSFT 5.0"** 适用于所有Windows 2000客户端（及更高版本）
- **"MSFT 98"** 适用于所有Windows 98和Me客户端
- **"MSFT"** 适用于所有Windows 98、Me和2000客户端

默认情况下，Apple MacBook设备不会发送选项60。

从Windows 10客户端捕获数据包的示例：

```
Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
```

3.选项55 — 参数请求列表

DHCP Parameter Request List选项包含DHCP客户端向DHCP服务器请求的配置参数（选项代码）。它是以逗号分隔记法书写的字符串（例如1,15,43）。

它不是一个完美的解决方案，因为它生成的数据取决于供应商，并且可以通过多种设备类型进行复制。

例如，默认情况下，Windows 10设备始终请求特定参数列表。Apple iPhone和iPad使用不同的参数集，可以在这些参数集上进行分类。

从Windows 10客户端捕获的示例：

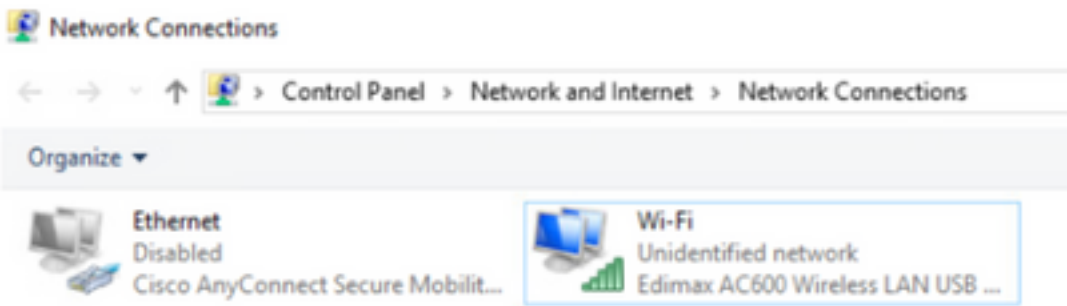
```
Option: (55) Parameter Request List
    Length: 14
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
```

4.选项77 — 用户类

User class是默认情况下最常使用的选项，需要手动配置客户端。例如，可以在windows计算机上使用以下命令配置此选项：

```
ipconfig /setclassid “ADAPTER_NAME” “USER_CLASS_STRING”
```

适配器名称可在控制面板中的“网络和共享中心”中找到：



在CMD中为Windows 10客户端配置DHCP选项66（需要管理员权限）：

```
C:\Windows\system32>ipconfig /setclassid "Wi-Fi" "test_user_class"

Windows IP Configuration

Successfully set the DHCPv4 class id for adapter Wi-Fi.
```

由于Windows实施了选项66,wireshark无法解码此选项，选项66之后的部分数据包显示为格式不正确：

```
  ⌄ Option: (77) User Class Information
      Length: 15
    ⌄ Instance of User Class: [0]
        User Class Length: 116
⌄ [Malformed Packet: DHCP/BOOTP]
  ⌄ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]
```

HTTP分析

HTTP分析是分析9800 WLC支持的最高级方法，它提供了最详细的设备分类。

对于要进行HTTP分析的客户端，它需要处于“运行”状态并执行HTTP GET请求。

WLC会拦截请求，并检查数据包的HTTP报头中的“User-Agent”字段。

此字段包含可用于对无线客户端进行分类的其他信息。

默认情况下，几乎所有制造商都实施了无线客户端尝试执行Internet连接检查的功能。

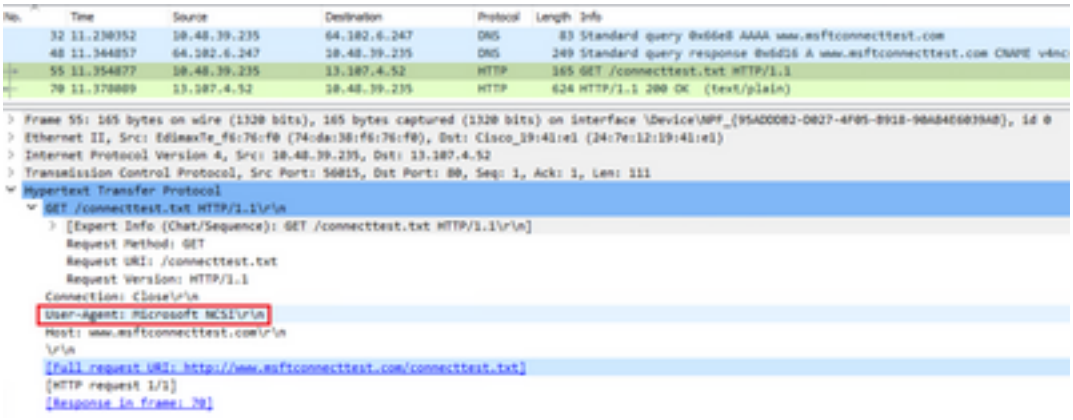
此检查也用于自动访客门户检测。 如果设备收到状态代码为200(OK)的HTTP响应，则表示未使用webauth保护WLAN。

如果是，则WLC执行必要的拦截，以执行身份验证的其余部分。 此初始HTTP GET不是唯一一个WLC可用于分析设备。

每个后续HTTP请求都由WLC检测，并且可能会产生更详细的分类。

Windows 10设备使用域**msftconnecttest.com**执行此测试。Apple设备使用**captive.apple.com**，而Android设备通常使用**connectivitycheck.gstatic.com**。

执行此检查的Windows 10客户端的数据包捕获可在下面找到。User Agent（用户代理）字段填充了**Microsoft NCSI**，这导致在WLC上客户端被分析为**Microsoft-Workstation**:



对于通过HTTP分析的客户端，**show wireless client mac-address [MAC_ADDR]**的详细示例输出：

```
Device Type       : Microsoft-Workstation
Device Name       : MSFT 5.0
Protocol Map      : 0x000029  (OUI, DHCP, HTTP)
Device OS         : Windows NT 10.0; Win64; x64; rv:76.0
Protocol          : HTTP
```

RADIUS分析

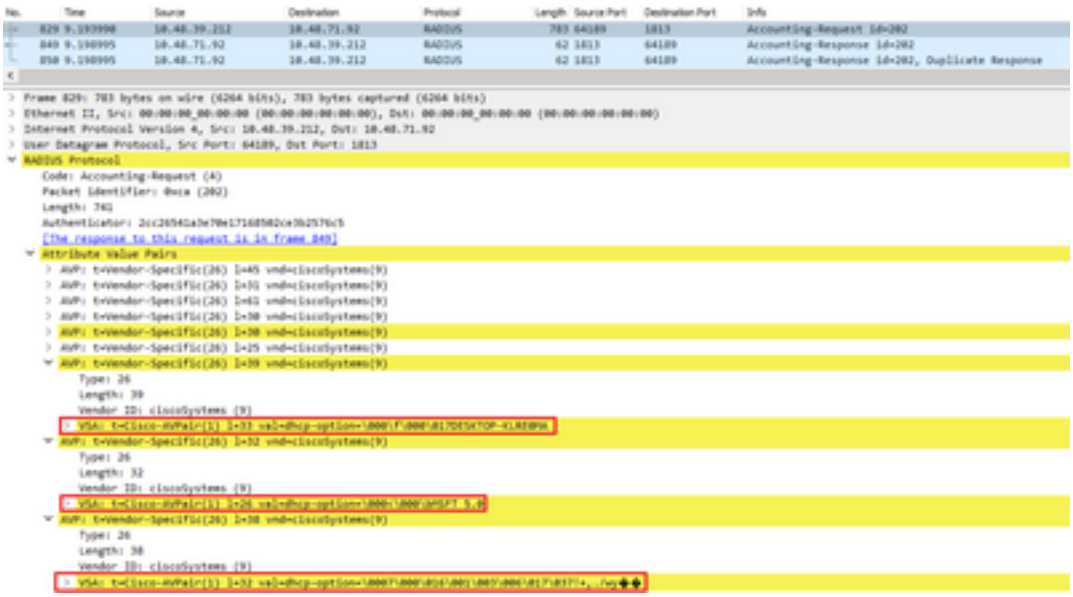
当涉及用于设备分类的方法时，本地和RADIUS分析没有区别。

如果启用了Radius分析，则WLC会通过一组特定供应商特定的RADIUS属性将其了解到的设备信息转发到RADIUS服务器。

DHCP RADIUS分析

通过DHCP分析获取的信息将作为供应商特定的RADIUS AVPair发送到记帐请求内的RADIUS服务器 **cisco-av-pair:dhcp-option=<DHCP选项>**

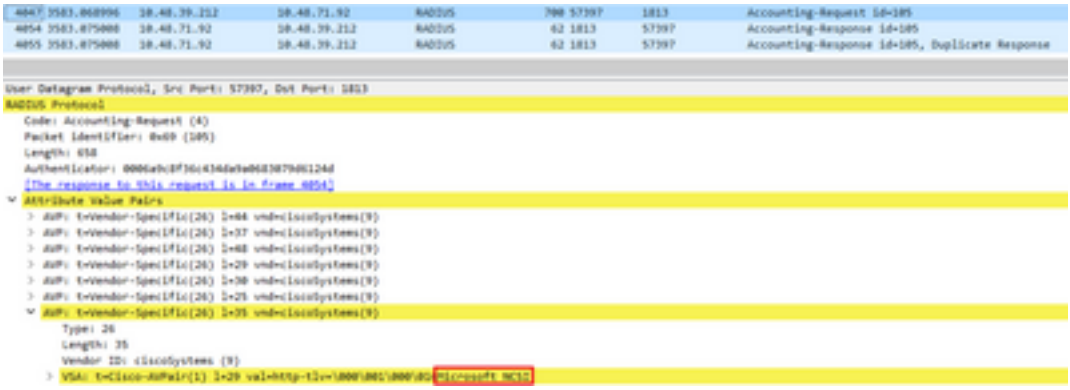
显示DHCP选项12、60和55的AVPairs的记帐请求数据包示例，分别从WLC发送到RADIUS服务器（选项55值可能因Wireshark解码而损坏）：



HTTP RADIUS分析

通过HTTP分析获取的信息（来自HTTP GET请求报头的用户代理字段）作为供应商特定RADIUS AVPair发送到记帐请求内部的RADIUS服务器 **cisco-av-pair:http-tlv=User-Agent=<user-agent>**

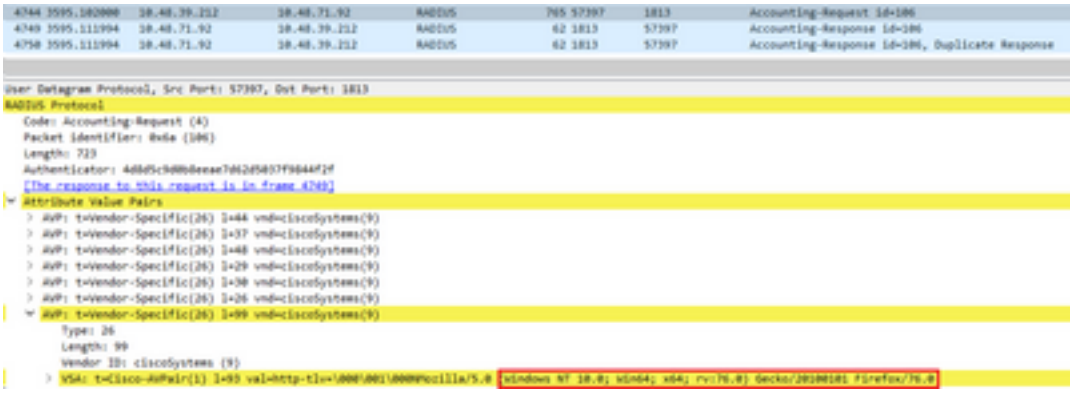
初始连接检查HTTP GET数据包在User-Agent字段中不包含太多信息，只有“Microsoft NCSI”。将此简单值转发到RADIUS服务器的记帐数据包示例：



一旦用户开始浏览Internet并创建一些额外的HTTP GET请求，就有可能获得有关它的更多信息。

如果检测到此客户端的新用户代理值，WLC会向ISE发送其他记帐数据包。

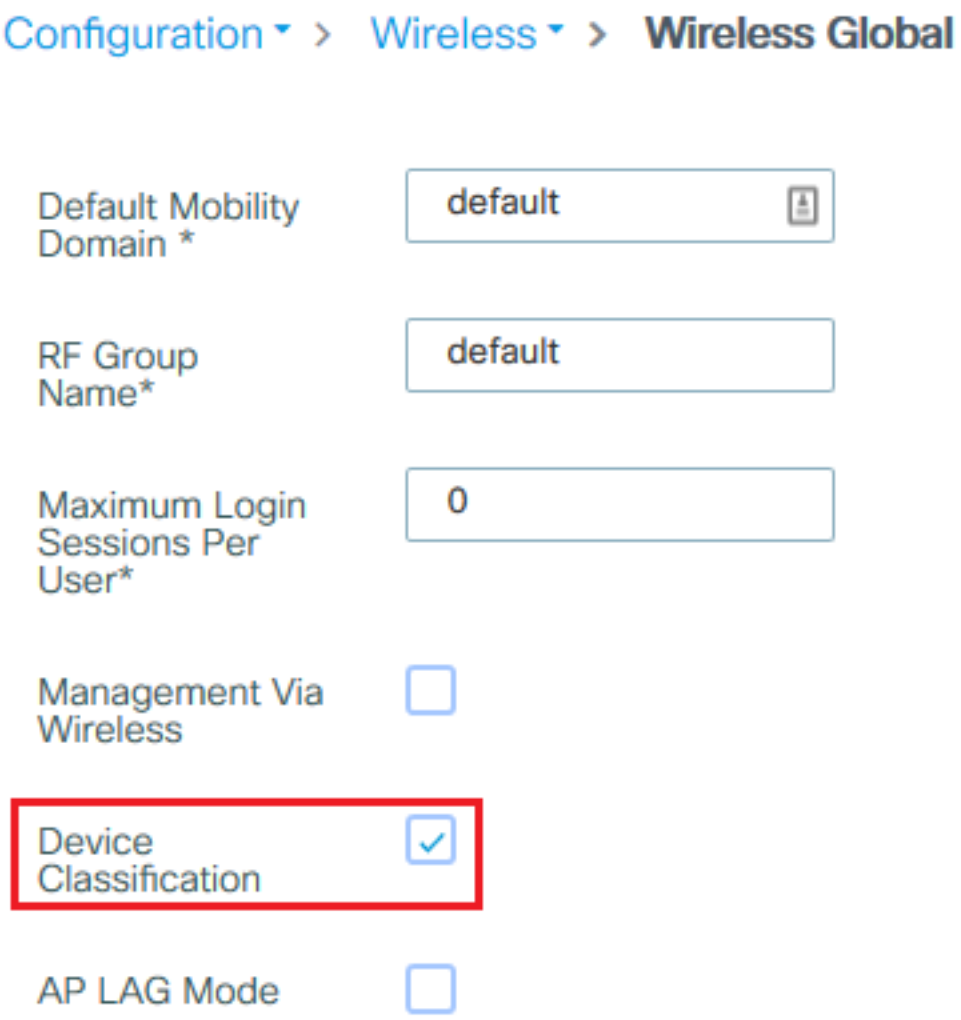
在本示例中，可以看到客户端使用Windows 10 64位和Firefox 76:



在9800 WLC上配置分析

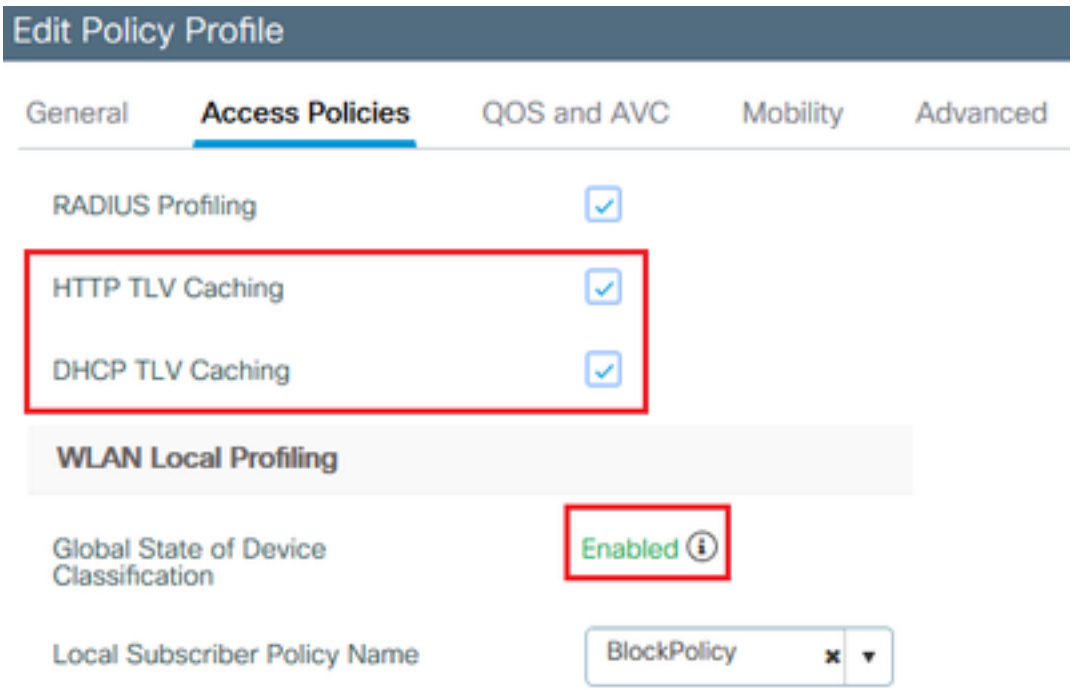
本地分析配置

为了使Local分析正常工作，只需在Configuration > Wireless > Wireless Global下启用Device Classification。此选项同时启用MAC OUI、HTTP和DHCP分析：



此外，在Policy configuration（策略配置）下，您可以启用HTTP TLV Caching（HTTP TLV缓存）和DHCP TLV Caching（DHCP TLV缓存）。即使没有配置文件，WLC也会执行分析。

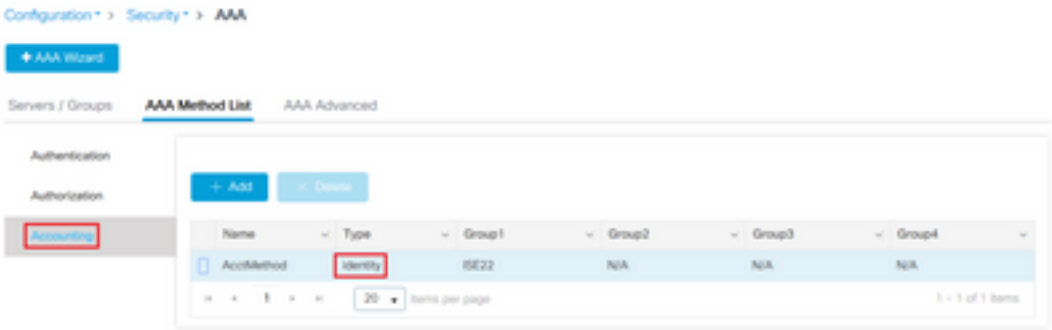
启用这些选项后，WLC将缓存以前了解的此客户端信息，并避免检查此设备生成的其他数据包。



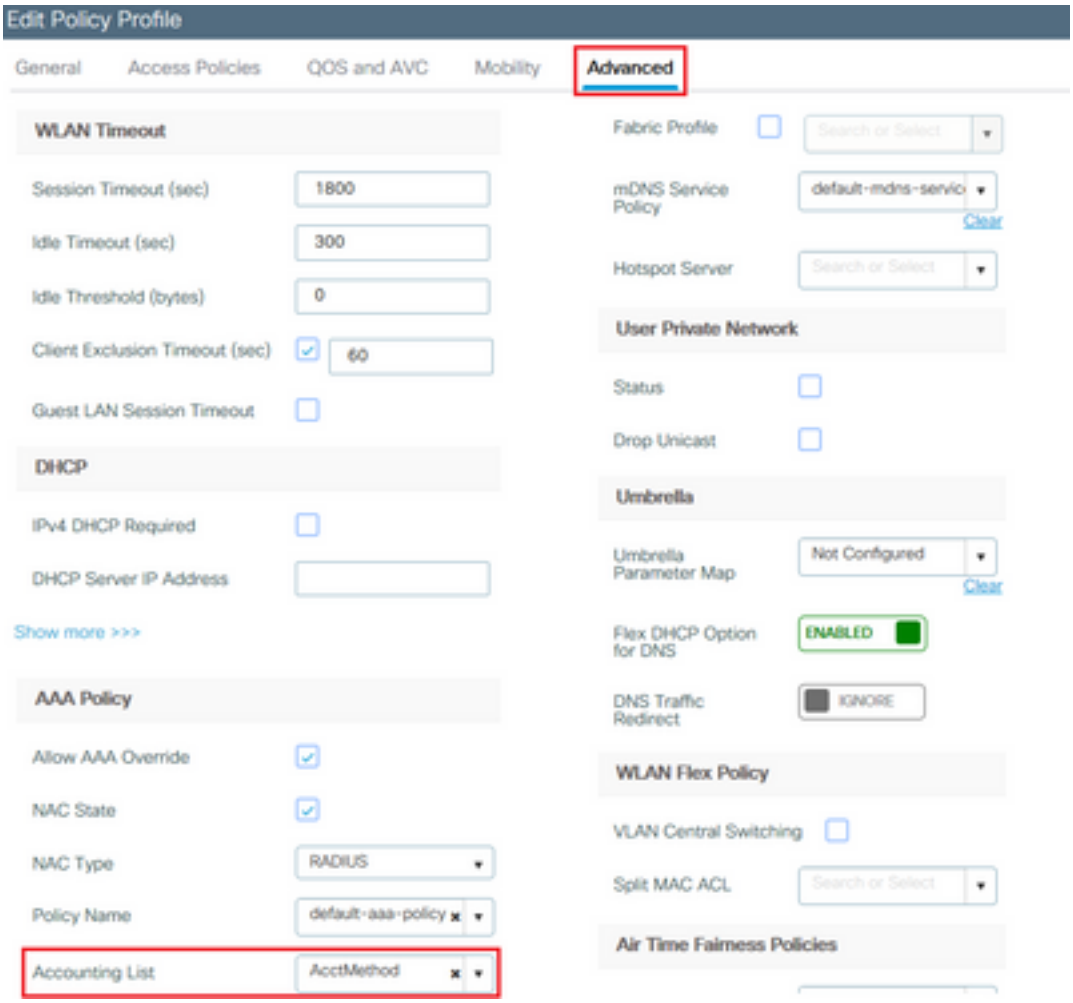
RADIUS分析配置

要使RADIUS分析生效，除了全局启用设备分类（如本地分析配置中所述），还需要：

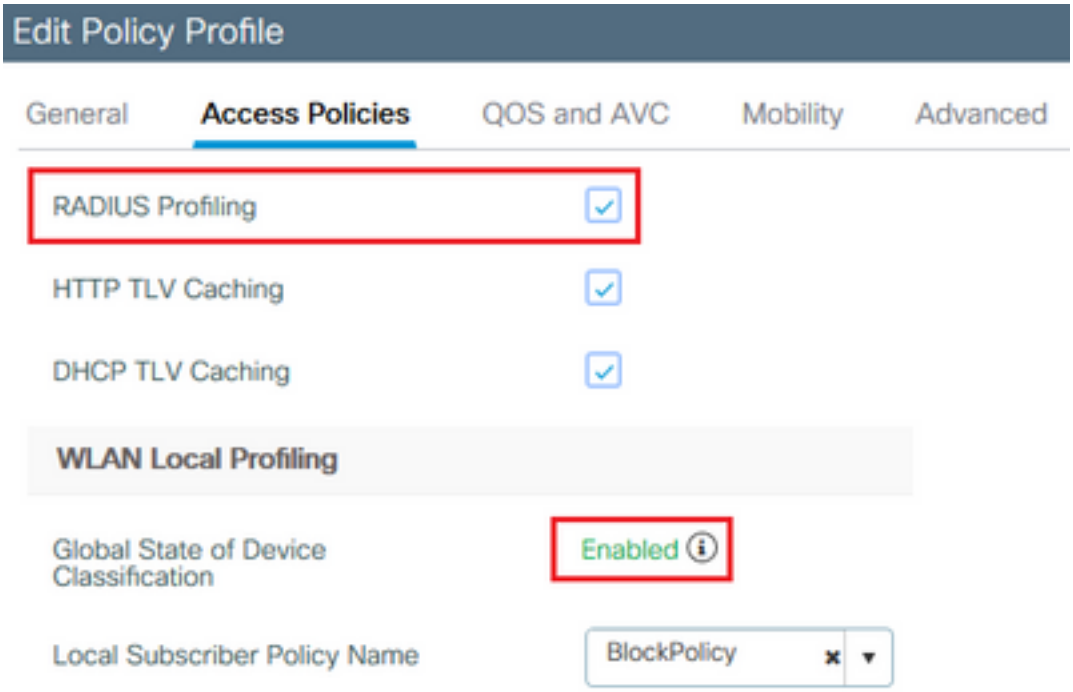
1.使用指向RADIUS服务器的“身份”类型配置AAA记帐方法：



2.需要在Configuration > Tags & Profiles > Policy > [Policy_Name] > Advanced下添加会计方法：



3.最后，需要在Configuration > Tags & Profiles > Policy下勾选RADIUS Profiling复选框此复选框启用HTTP和DHCP RADIUS分析（旧的AireOS WLC有2个单独的复选框）：



分析使用案例

基于本地分析分类应用本地策略

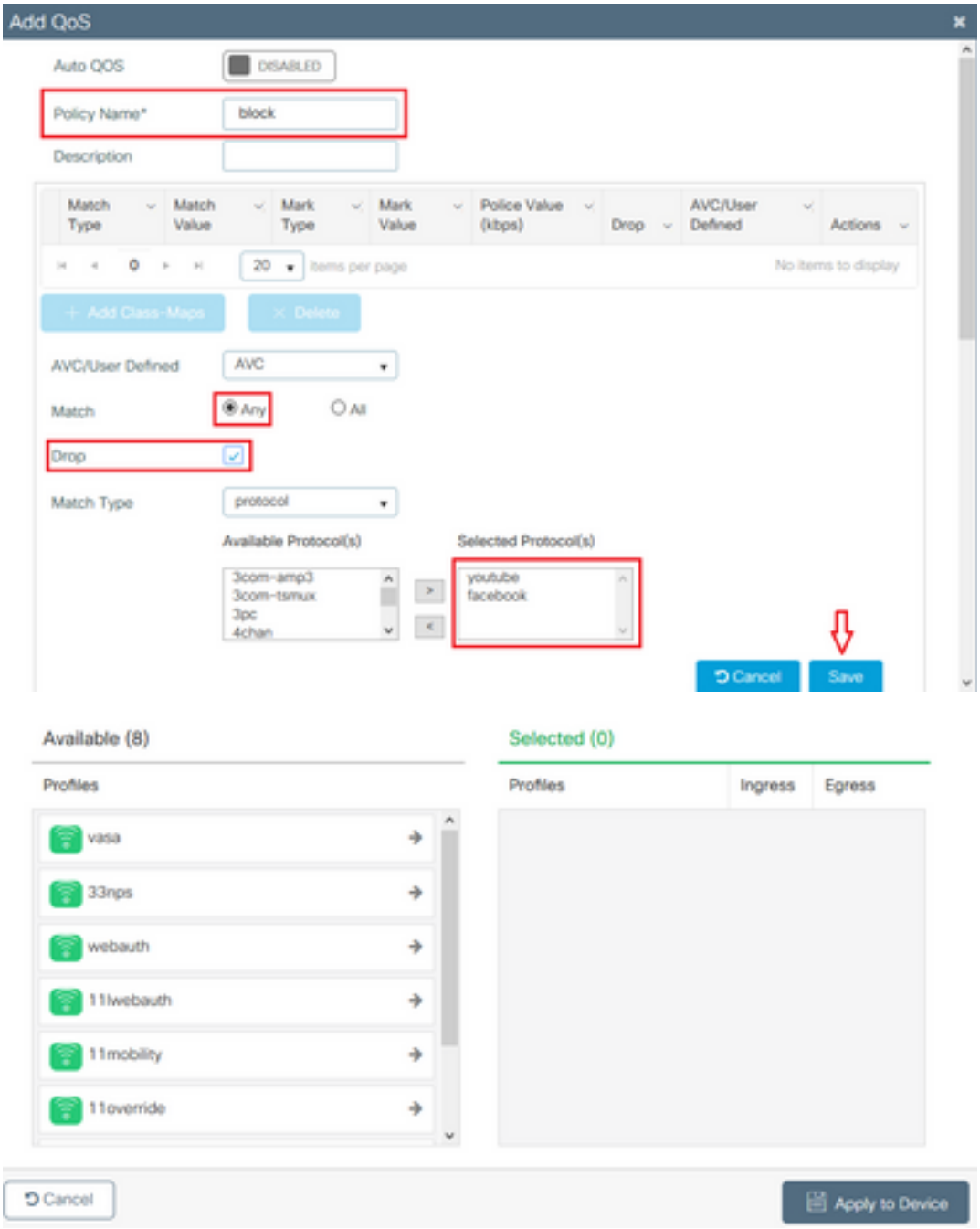
此示例配置演示了本地策略的配置，该本地策略具有QoS配置文件阻止youtube和facebook访问，仅应用于被分析为Windows-Workstation的设备。

只需稍作更改，即可修改此配置，例如，仅对无线电话设置特定DSCP标记。

导航到**配置 > 服务 > QoS**以创建QoS配置文件。点击add以创建新策略：

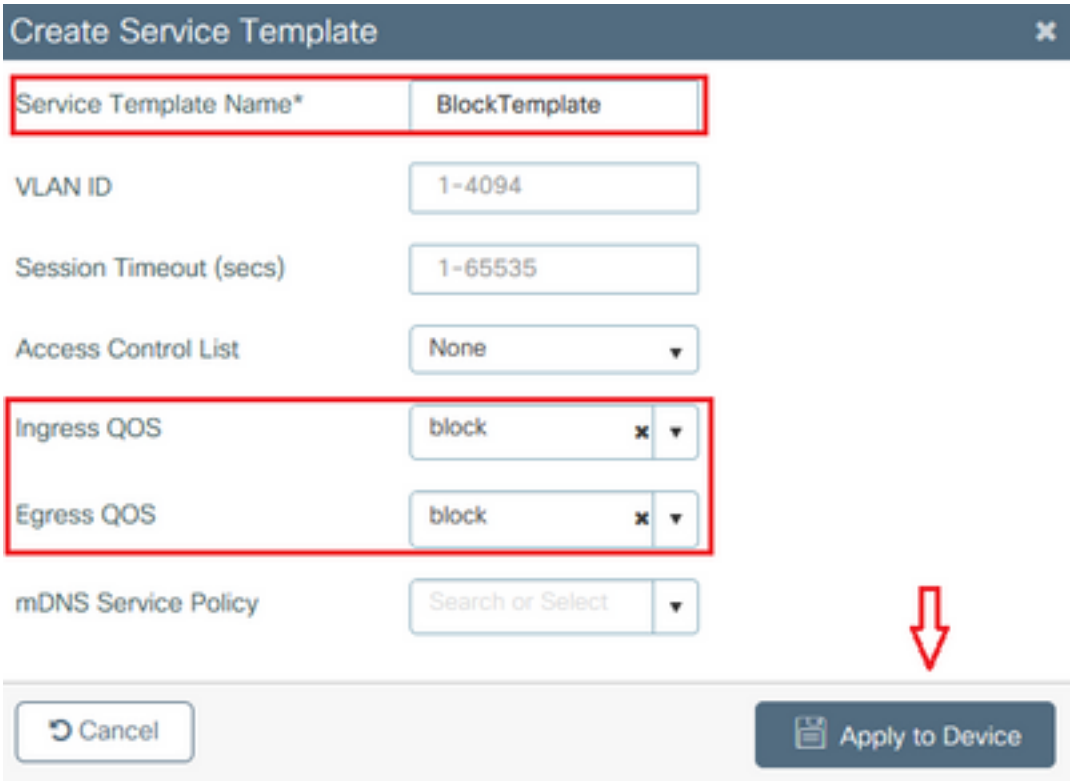
指定策略名称并添加新的类映射。从可用协议中，选择需要被阻止、已标记DSCP或已限制带宽的协议。

在本例中，youtube和facebook被阻止。请确保不将此QoS配置文件应用于QoS窗口底部的任何策略配置文件：

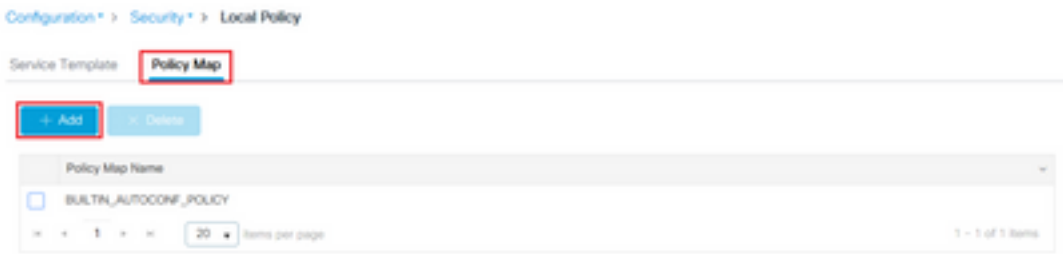


导航到**Configuration > Security > Local Policy**并创建新的服务模板：

指定在上一步中创建的入口和出口QoS配置文件。在此步骤中还可以应用访问列表。如果无需更改VLAN，请将vlan字段留空：



导航到Policy Map选项卡，然后点击add:

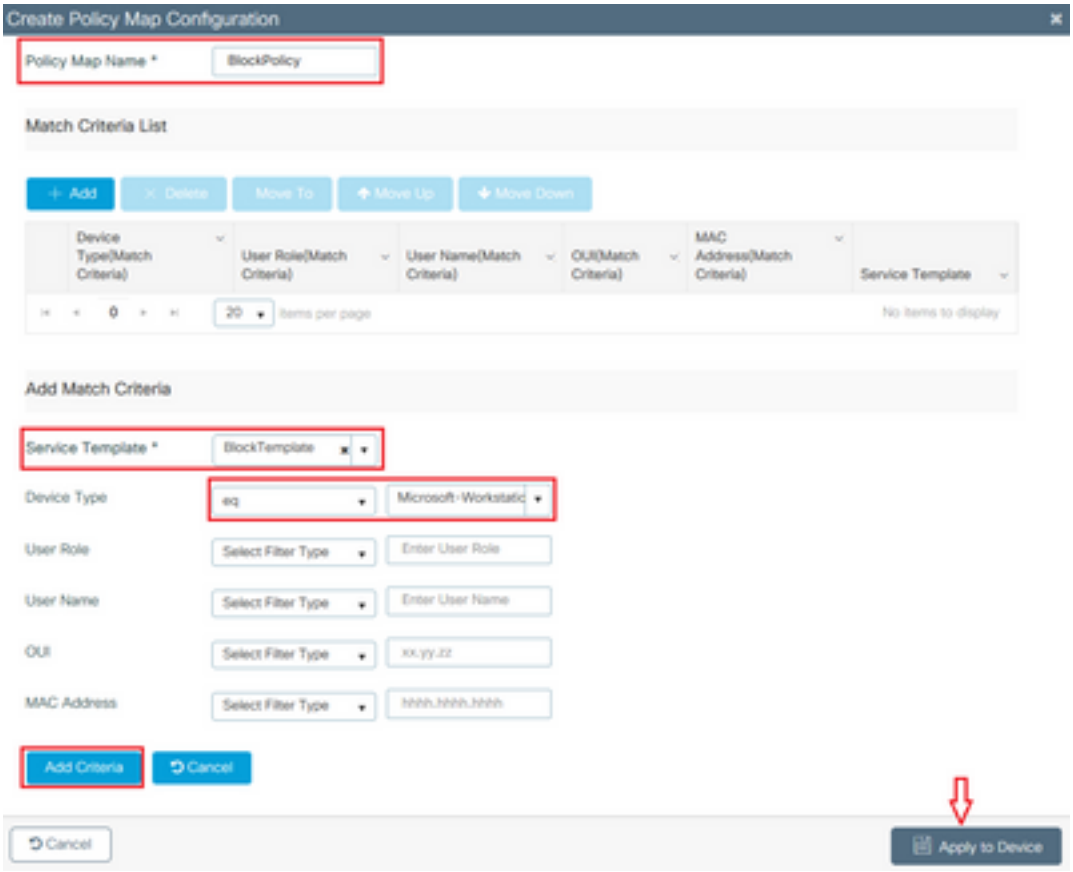


设置策略映射名称并添加新条件。指定在上一步中创建的服务模板，并选择应用此模板的设备类型。

在本例中，使用Microsoft-Workstation。如果定义了多个策略，则使用第一个匹配项。

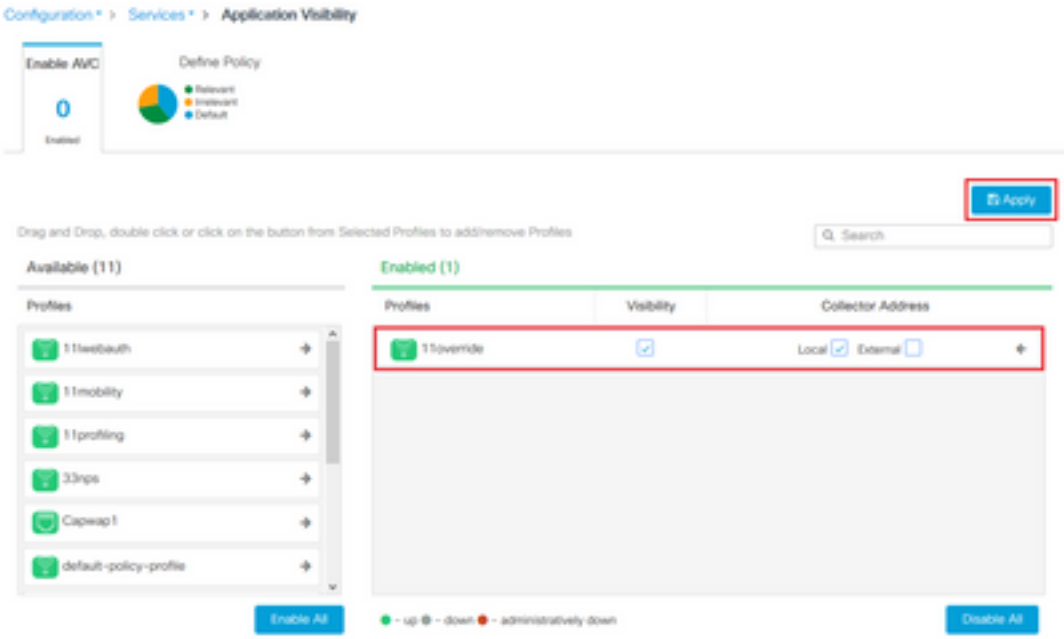
另一个常见使用案例是指定基于OUI的匹配条件。如果部署具有大量相同型号的扫描仪或打印机，它们通常具有相同的MAC OUI。

这可用于应用特定QoS DSCP标记或ACL:

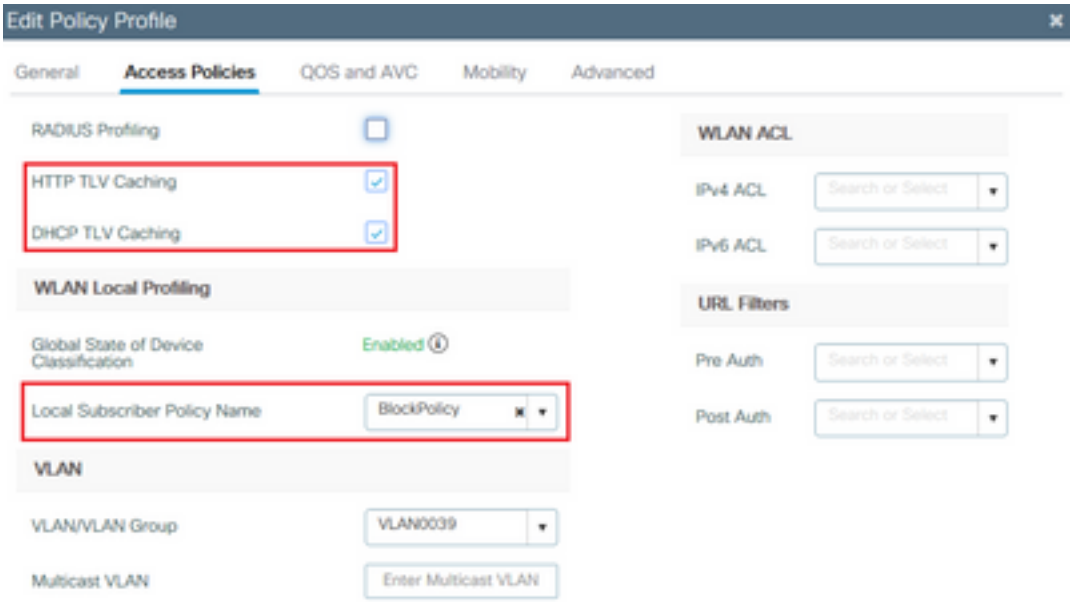


为了使WLC能够识别youtube和facebook流量，需要打开应用可视性。

导航到**配置 > 服务 > 应用可视性** e对您的WLAN的策略配置文件启用可视性：



验证在策略Profile下，已启用HTTP TLV缓存、DHCP TLV缓存、全局设备分类，并且本地用户策略指向在以上步骤之一中创建的本地策略映射：



客户端连接后，可以检查是否已应用本地策略，并测试youtube和facebook是否实际被阻止。

show wireless client mac-address [MAC_ADDR] detailed的输出包括：

```
Input Policy Name  : block
Input Policy State : Installed
Input Policy Source : Native Profile Policy
Output Policy Name  : block
Output Policy State : Installed
Output Policy Source : Native Profile Policy

Local Policies:
  Service Template : BlockTemplate (priority 150)
  Input QOS        : block
  Output QOS       : block
  Service Template : wlan_svc_11override_local (priority 254)
  VLAN             : VLAN0039
  Absolute-Timer   : 1800

Device Type      : Microsoft-Workstation
Device Name      : MSFT 5.0
Protocol Map     : 0x000029  (OUI, DHCP, HTTP)
Protocol         : HTTP
```

思科ISE中的高级策略集的RADIUS分析

启用RADIUS分析后，WLC将分析信息转发到ISE。根据此信息，可以创建高级身份验证和授权规则。

本文不包括ISE配置。有关详细信息，请参阅Cisco ISE分析设计指南。

此工作流程通常需要使用CoA，因此请确保在9800 WLC上启用此工作流程。

FlexConnect部署中的分析

集中身份验证、本地交换

在此设置中，本地和RADIUS分析继续按前几章所述工作。如果AP进入独立模式（AP失去与WLC的连接），设备分析将停止工作，并且没有新的客户端能够连接。

本地身份验证、本地交换

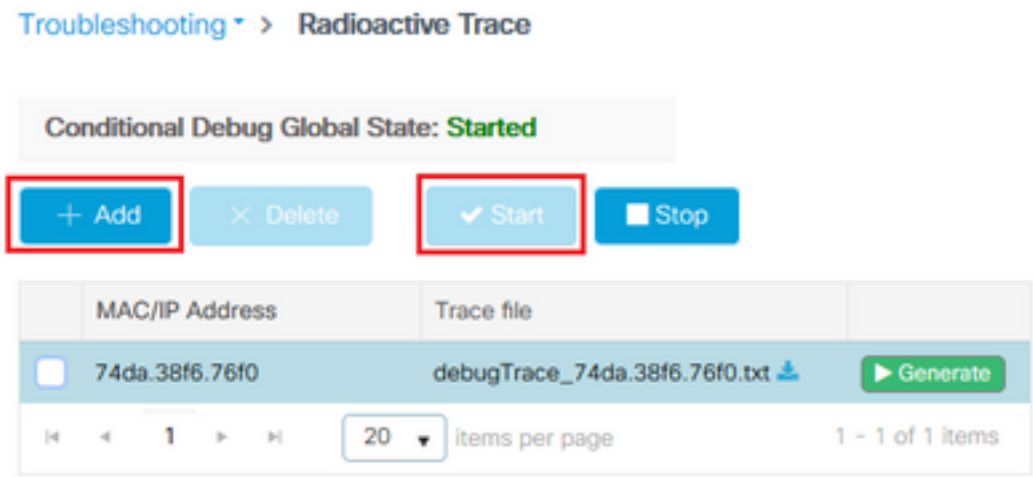
如果AP处于连接模式（AP加入到WLC），分析将继续工作（AP将客户端DHCP数据包的副本发送到WLC以执行分析过程）。

尽管分析工作正常，但由于身份验证在AP上本地执行，因此分析信息不能用于任何本地策略配置或RADIUS分析规则。

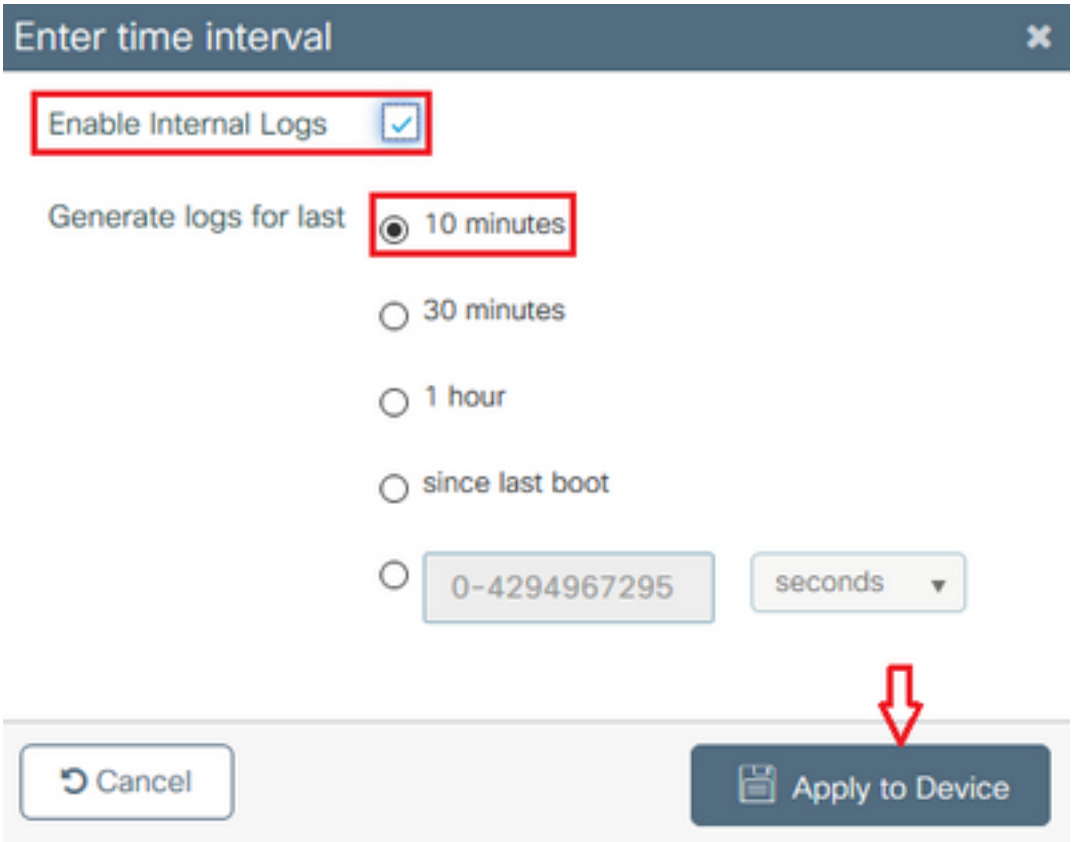
故障排除

放射性痕迹

排除WLC上的客户端配置文件故障的最简单方法是使用放射性跟踪。导航到**故障排除 > 放射跟踪**，输入客户端无线适配器MAC地址，然后点击“开始”：



将客户端连接到网络，并等待它达到运行状态。停止跟踪，然后单击**Generate**。确保启用内部日志（此选项仅存在于17.1.1版本及更高版本中）：



放射性痕迹的相关片段可在以下位置找到：

WLC将客户端分析为Microsoft-Workstation:

```
2020/06/18 10:46:41.052366 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (info):
[74da.38f6.76f0:capwap_90000004] Device type for the session is detected as Microsoft-
Workstation and old device-type not classified earlier &Device name for the session is detected
as MSFT 5.0 and old device-name not classified earlier & Old protocol map 0 and new is 41
2020/06/18 10:46:41.052367 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (debug):
[74da.38f6.76f0:capwap_90000004] updating device type Microsoft-Workstation, device name MSFT
5.0
```

WLC缓存设备分类：

```
(debug): [74da.38f6.76f0:unknown] Updating cache for mac [74da.38f6.76f0] device_type:
Microsoft-Workstation, device_name: MSFT 5.0 user_role: NULL protocol_map: 41
```

WLC在缓存中查找设备分类：

```
(info): [74da.38f6.76f0:capwap_90000004] Device type found in cache Microsoft-Workstation
```

WLC应用基于分类的本地策略：

```
(info): device-type filter: Microsoft-Workstation required, Microsoft-Workstation set - match
for 74da.38f6.76f0 / 0x9700001A
(info): device-type Filter evaluation succeeded
(debug):  match device-type eq "Microsoft-Workstation" :success
```

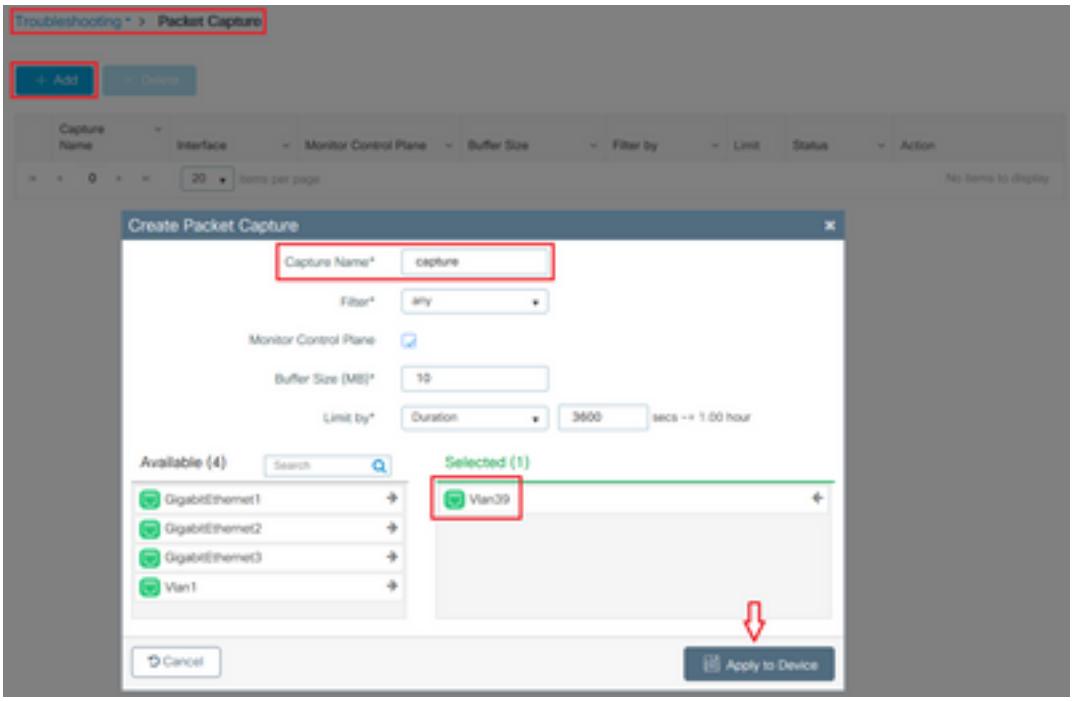
WLC发送包含DHCP和HTTP分析属性的记帐数据包：

```
[caaa-acct] [21168]: (debug): [CAAA:ACCT:c9000021] Accounting session created
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Getting active filter list
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found http
[auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_90000004] Found dhcp
[aaa-attr-inf] [21168]: (debug): Filter list http-tlv 0
[aaa-attr-inf] [21168]: (debug): Filter list dhcp-option 0

[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-profile-name 0 "Microsoft-Workstation"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-name 0 "MSFT 5.0"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-class-tag 0 "Workstation:Microsoft-
Workstation"
[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-certainty-metric 0 10 (0xa)
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 0c 00 0f 44 45 53 4b 54 4f 50
2d 4b 4c 52 45 30 4d 41
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 3c 00 08 4d 53 46 54 20 35 2e
30
[aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 37 00 0e 01 03 06 0f 1f 21 2b
2c 2e 2f 77 79 f9 fc

### http profiling sent in a separate accounting packet
[aaa-attr-inf] [21168]: (debug): Get acct attrs http-tlv 0 00 01 00 0e 4d 69 63 72 6f 73 6f 66
74 20 4e 43 53 49
```

数据包捕获

在集中交换部署中，可以在WLC本身上执行数据包捕获。导航到**故障排除 > Packet Capture**，并在此客户端正在使用的其中一个接口上创建新的捕获点。

需要在vlan上具有SVI才能对其执行捕获，否则需要在物理端口本身上捕获数据



关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。