

演示9800無線LAN控制器上的客戶端效能分析

目錄

[簡介](#)

[採用元件](#)

[分析過程](#)

[MAC地址OUI分析](#)

[本地管理的MAC地址問題](#)

[DHCP分析](#)

[HTTP分析](#)

[RADIUS分析](#)

[DHCP RADIUS分析](#)

[HTTP RADIUS分析](#)

[在9800 WLC上配置效能分析](#)

[本地分析配置](#)

[RADIUS分析配置](#)

[分析使用案例](#)

[基於區域性特徵分類的應用區域性策略](#)

[思科ISE高級策略集的RADIUS分析](#)

[在FlexConnect部署中進行分析](#)

[集中身份驗證、本地交換](#)

[本地身份驗證、本地交換](#)

[疑難排解](#)

[放射性痕跡](#)

[封包擷取](#)

簡介

本檔案將說明裝置分類和分析在Cisco Catalyst 9800無線LAN控制器上的運作方式。

採用元件

- 執行17.2.1映像的9800 CL WLC
- 1815i存取點
- Windows 10 Pro無線客戶端
- Cisco ISE 2.7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

分析過程

本文深入瞭解裝置分類和分析在Cisco Catalyst 9800無線LAN控制器上的運作方式，介紹潛在的使用案例、組態範例，以及進行疑難排解的必要步驟。

裝置分析是一種功能，可用於查詢有關已加入無線基礎設施的無線客戶端的其他資訊。

執行裝置分析後，可使用它來應用不同的本地策略或匹配特定的RADIUS伺服器規則。

Cisco 9800 WLC能夠執行三(3)種型別的裝置分析：

1. MAC地址OUI
2. DHCP
3. HTTP

MAC地址OUI分析

MAC地址是每個無線（和有線）網路介面的唯一識別符號。這是一個通常以十六進位制格式MM:MM:MM:SS:SS:SS寫下的48位數字。

前24位（或3個二進位制八位數）稱為OUI（組織唯一識別符號），它們唯一標識供應商或製造商。

它們由IEEE購買和分配。一個供應商或製造商可以購買多個OUI。

範例：

00:0D:4B - owned by Roku, LLC

90:78:B2 - owned by Xiaomi Communications Co Ltd

無線客戶端與接入點關聯後，WLC會執行OUI查詢以確定製造商。

在Flexconnect本地交換部署中，AP仍會將相關的客戶端資訊中繼到WLC（例如DHCP資料包和客戶端mac地址）。

僅基於OUI的特徵提取極為有限，可以將裝置分類為特定品牌，但無法區分筆記型電腦和智慧手機。

本地管理的MAC地址問題

出於隱私考慮，許多製造商開始在他們的裝置上實施MAC隨機化功能。

本地管理的MAC地址是隨機生成的，並且地址第一八位數的第二最低有效位設定為1。

此位充當一個標誌，用於宣佈mac地址實際上是一個隨機生成的地址。

本地管理的MAC地址有四種可能的格式（x可以是任何十六進位制值）：

x2-xx-xx-xx-xx-xx

x6-xx-xx-xx-xx-xx

xA-xx-xx-xx-xx-xx

xE-xx-xx-xx-xx-xx

預設情況下，Android 10裝置在每次連線到新的SSID網路時使用隨機生成的本地管理的MAC地址。

由於控制器識別出地址是隨機化的，並且不執行任何查詢，因此此功能完全破壞了基於OUI的裝置分類。

DHCP分析

DHCP分析由WLC通過調查無線客戶端發出的DHCP資料包來執行。

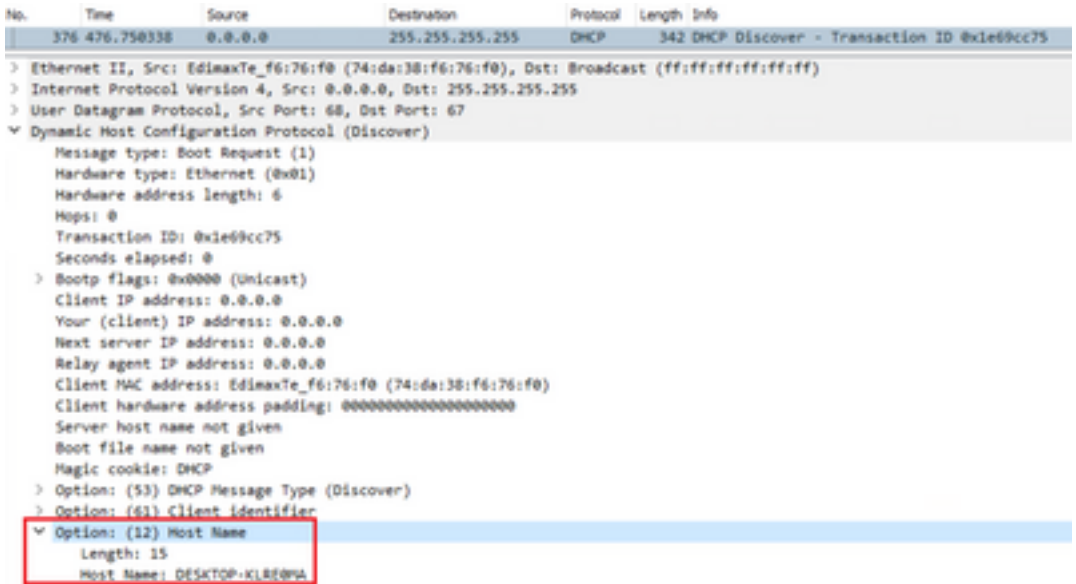
如果使用DHCP分析對裝置進行分類，`show wireless client mac-address [MAC_ADDR] detailed`命令的輸出包括：

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

WLC會檢查無線使用者端傳送的封包中的多個DHCP選項欄位：

1. 選項12 — 主機名

此選項表示客戶端主機名，可在DHCP發現和DHCP請求資料包中找到：



```
No.    Time           Source            Destination      Protocol  Length  Info
376 476.750338    0.0.0.0          255.255.255.255  DHCP     342    DHCP Discover - Transaction ID 0x1e69cc75
> Ethernet II, Src: EdimaxTe_f6:76:f0 (74:da:38:f6:76:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x1e69cc75
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: EdimaxTe_f6:76:f0 (74:da:38:f6:76:f0)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client Identifier
  v Option: (12) Host Name
    Length: 15
    Host Name: DESKTOP-KL8F0M4
```

2. 選項60 — 供應商類別識別符號

也可以在DHCP發現和請求資料包中找到此選項。

使用此選項，客戶端可以向DHCP伺服器標識自己，然後可以將伺服器配置為僅響應具有特定供應商類別識別符號的客戶端。

此選項最常用於標識網路中的接入點，並且僅使用選項43對其作出響應。

供應商類識別符號示例

- "MSFT 5.0" 適用於所有Windows 2000客戶端 (及更高版本)
- 「MSFT 98」 適用於所有Windows 98和Me客戶端
- "MSFT" 適用於所有Windows 98、Me和2000客戶端

預設情況下，Apple MacBook裝置不會傳送選項60。

從Windows 10客戶端捕獲資料包的示例：

Option: (60) Vendor class identifier

Length: 8

Vendor class identifier: MSFT 5.0

3. 選項55 — 引數請求清單

DHCP Parameter Request List 選項包含DHCP客戶端向DHCP伺服器請求的配置引數 (選項代碼)。它是以逗號分隔的記法編寫的字串 (例如1,15,43)。

這不是一個完美的解決方案，因為它生成的資料取決於供應商，可以按多種裝置型別進行複製。

例如，預設情況下，Windows 10裝置總是請求特定引數清單。蘋果iPhone和iPad使用不同的參陣列合，可以對它們進行分類。

從Windows 10客戶端捕獲的示例：

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)

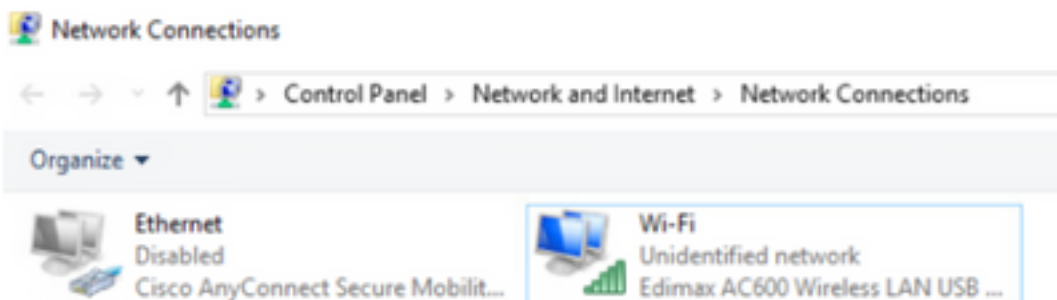
Parameter Request List Item: (252) Private/Proxy autodiscovery

4. 選項77 — 使用者類

使用者類是預設情況下最常使用的選項，需要手動配置客戶端。例如，可以在Windows電腦上使用以下命令配置此選項：

```
ipconfig /setclassid "ADAPTER_NAME" "USER_CLASS_STRING"
```

介面卡名稱可在控制面板中的「網路和共用中心」中找到：



在CMD中為Windows 10客戶端配置DHCP選項66 (需要管理員許可權)：

```
C:\Windows\system32>ipconfig /setclassid "Wi-Fi" "test_user_class"
Windows IP Configuration
Successfully set the DHCPv4 class id for adapter Wi-Fi.
```

由於Windows實施了選項66,wireshark無法解碼此選項，選項66之後到達的部分資料包顯示為格式不正確：

```
  ▾ 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支援的最高級方法，它提供了最詳細的裝置分類。

對於要進行HTTP分析的客戶端，它需要處於「運行」狀態並執行HTTP GET請求。

WLC會攔截該要求並檢查封包的HTTP標頭中的「User-Agent」欄位。

此欄位包含有關可用於對其進行分類的無線客戶端的其他資訊。

預設情況下，幾乎所有製造商都實施了無線客戶端嘗試執行網際網路連線檢查的功能。

此檢查也用於自動訪客門戶檢測。如果裝置收到狀態碼為200(OK)的HTTP回應，則表示沒有使用webauth來保護WLAN。

如果均為0,WLC會執行執行其餘驗證所需的偵聽。此初始HTTP GET不是唯一一個WLC可用於設定裝置設定檔的。

WLC會檢查每個後續的HTTP要求，而且可能會產生更詳細的分類。

Windows 10裝置使用域msftconnecttest.com執行此測試。Apple裝置使用captive.apple.com，而Android裝置通常使用connectivitycheck.gstatic.com。

執行此檢查的Windows 10客戶端的資料包捕獲可在下面找到。「使用者代理」欄位填充了Microsoft NCSI，這導致在WLC上將客戶端配置為Microsoft-Workstation:

```

No.    Time    Source          Destination     Protocol  Length  Info
---    -
32    11.238752  10.40.39.235   64.182.6.247   DNS       83      Standard query 0xb6e8 AAAA www.msftconnecttest.com
48    11.344857  64.182.6.247   10.40.39.235   DNS       249     Standard query response 0xb6e8 A www.msftconnecttest.com CNAME v4nc
55    11.354877  10.40.39.235   13.107.4.52    HTTP      365     GET /connecttest.txt HTTP/1.1
70    11.370809  13.107.4.52    10.40.39.235   HTTP      624     HTTP/1.1 200 OK (text/plain)

> Frame 55: 365 bytes on wire (1320 bits), 365 bytes captured (1320 bits) on interface \Device\NPF_{954DCC0B2-0B27-4F05-8918-96A84E6839A8}, id 0
> Ethernet II, Src: EdimaxFe_f6:76:c0 (74:6d:a3:81:f6:76:c0), Dst: Cisco_39:41:e1 (24:7e:12:19:41:e1)
> Internet Protocol Version 4, Src: 10.40.39.235, Dst: 13.107.4.52
> Transmission Control Protocol, Src Port: 50015, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol
  GET /connecttest.txt HTTP/1.1\r\n
  > [Expert Info (Chat/Sequence): GET /connecttest.txt HTTP/1.1\r\n
  Request Method: GET
  Request URI: /connecttest.txt
  Request Version: HTTP/1.1
  Connection: Close\r\n
  User-Agent: Microsoft NCSA\r\n
  Host: www.msftconnecttest.com\r\n
  \r\n
  [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
  [HTTP request 1/3]
  [Response in frame: 70]

```

對於通過HTTP分析的客戶端，show wireless client mac-address [MAC_ADDR]的輸出示例是詳細的：

```

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

當涉及用於裝置分類的方法時，本地和RADIUS分析之間沒有區別。

如果啟用Radius分析，WLC會將它透過一組特定廠商的RADIUS屬性所瞭解的裝置資訊轉送到RADIUS伺服器。

DHCP RADIUS分析

通過DHCP分析獲取的資訊將作為特定於供應商的RADIUS AVPair傳送到記帳請求內部的RADIUS伺服器 `cisco-av-pair:dhcp-option=<DHCP選項>`

顯示DHCP選項12、60和55的AVPairs的記帳請求資料包的示例，分別從WLC傳送到RADIUS伺服器（選項55值可能由於Wireshark解碼而損壞）：

```

No.    Time    Source          Destination     Protocol  Length  Source Port  Destination Port  Info
---    -
829    9.193996  10.40.39.212   10.40.71.92    RADIUS    783    64189        1813              Accounting-Request Id=262
849    9.198995  10.40.71.92    10.40.39.212   RADIUS    62      1813         64189             Accounting-Response Id=262
850    9.198995  10.40.71.92    10.40.39.212   RADIUS    62      1813         64189             Accounting-Response Id=262, Duplicate Response

> Frame 829: 783 bytes on wire (3132 bits), 783 bytes captured (3132 bits)
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 10.40.39.212, Dst: 10.40.71.92
> User Datagram Protocol, Src Port: 64189, Dst Port: 1813
RADIUS Protocol
  Code: Accounting-Request (4)
  Packet Identifier: 0xa (262)
  Length: 783
  Authenticator: 21c269404b70e17168502c3062576c5
  [The response to this request is in frame 849]
  Attribute Value Pairs
  > AVP: t=vendor-specific(26) l=45 vnd=cisco-system(9)
  > AVP: t=vendor-specific(26) l=30 vnd=cisco-system(9)
  > AVP: t=vendor-specific(26) l=60 vnd=cisco-system(9)
  > AVP: t=vendor-specific(26) l=38 vnd=cisco-system(9)
  > AVP: t=vendor-specific(26) l=38 vnd=cisco-system(9)
  > AVP: t=vendor-specific(26) l=25 vnd=cisco-system(9)
  > AVP: t=vendor-specific(26) l=39 vnd=cisco-system(9)
  Type: 26
  Length: 39
  Vendor ID: cisco-system(9)
  > AVP: t=cisco-av-pair(1) l=33 vnd=+dhcp-option=1000:P.0000170DxTOP-CLASOPS
  > AVP: t=vendor-specific(26) l=32 vnd=cisco-system(9)
  Type: 26
  Length: 32
  Vendor ID: cisco-system(9)
  > AVP: t=cisco-av-pair(1) l=20 vnd=+dhcp-option=1000:P.00001007-3-C
  > AVP: t=vendor-specific(26) l=38 vnd=cisco-system(9)
  Type: 26
  Length: 38
  Vendor ID: cisco-system(9)
  > AVP: t=cisco-av-pair(1) l=37 vnd=+dhcp-option=1000:P.0000101000-0007.0000-017.01714-1-00-00

```

HTTP RADIUS分析

通過HTTP分析 (來自HTTP GET請求標頭的User-Agent欄位) 獲取的資訊將作為供應商特定的RADIUS AVPair傳送到記帳請求內部的RADIUS伺服器 `cisco-av-pair:http-tlv=User-Agent=<user-agent>`

初始連線檢查HTTP GET資料包在User-Agent欄位 (僅「Microsoft NCSI」) 中不包含太多資訊。將這個簡單值轉送到RADIUS伺服器的記帳封包範例：

```
4007 1583.875000  10.48.39.212  10.48.71.92  RADIUS  700 57397  1813  Accounting-Request Id=185
4054 1583.875000  10.48.71.92  10.48.39.212  RADIUS  62 1813  57397  Accounting-Response Id=185
4055 1583.875000  10.48.71.92  10.48.39.212  RADIUS  62 1813  57397  Accounting-Response Id=185, Duplicate Response

User Datagram Protocol, Src Port: 57397, Dest Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 0x09 (305)
Length: 658
Authenticator: 0000a0c0f36c434d4a6830794012ad
[The response to this request is in frame 4054]
Attribute Value Pairs
  AVP: t=Vendor-Specific(26) l=84 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=37 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=88 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=29 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=30 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=25 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=35 v=vdw:ciscoSystems(9)
    Type: 26
    Length: 35
    Vendor ID: ciscoSystems (9)
  VS: t=Cisco-AVPair(1) l=29 v=1-http-tlv=0000000000000000 [Microsoft NCSI]
```

使用者開始瀏覽Internet並建立一些額外的HTTP GET請求後，就可以獲得有關它的更多資訊。

如果檢測到此客戶端的新使用者代理值，WLC會向ISE傳送其他記帳資料包。

在此範例中，可以看到使用者端正在使用Windows 10 64位和Firefox 76:

```
4744 3595.111994  10.48.39.212  10.48.71.92  RADIUS  705 57397  1813  Accounting-Request Id=186
4749 3595.111994  10.48.71.92  10.48.39.212  RADIUS  62 1813  57397  Accounting-Response Id=186
4750 3595.111994  10.48.71.92  10.48.39.212  RADIUS  62 1813  57397  Accounting-Response Id=186, Duplicate Response

User Datagram Protocol, Src Port: 57397, Dest Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 0x0a (306)
Length: 723
Authenticator: 408d5c900b8eeae706245037f9844f2f
[The response to this request is in frame 4749]
Attribute Value Pairs
  AVP: t=Vendor-Specific(26) l=44 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=37 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=48 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=29 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=30 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=26 v=vdw:ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=99 v=vdw:ciscoSystems(9)
    Type: 26
    Length: 99
    Vendor ID: ciscoSystems (9)
  VS: t=Cisco-AVPair(1) l=93 v=1-http-tlv=0000000000000000 [Windows NT 10.0; Win64; x64; rv:76.0] Gecko/20100101 Firefox/76.0
```

在9800 WLC上配置效能分析

本地分析配置

為了使Local分析正常工作，只需在Configuration > Wireless > Wireless Global下啟用Device Classification。此選項同時啟用MAC OUI、HTTP和DHCP分析：

Default Mobility Domain *	<input type="text" value="default"/>
RF Group Name*	<input type="text" value="default"/>
Maximum Login Sessions Per User*	<input type="text" value="0"/>
Management Via Wireless	<input type="checkbox"/>
Device Classification	<input checked="" type="checkbox"/>
AP LAG Mode	<input type="checkbox"/>

此外，在Policy configuration (策略配置) 下，您可以啟用HTTP TLV Caching (HTTP TLV快取) 和DHCP TLV Caching (DHCP TLV快取)。即使沒有配置檔案，WLC也會執行效能分析。

啟用這些選項後，WLC會快取先前瞭解的此使用者端資訊，並避免檢查此裝置產生的其他封包。

Edit Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling	<input checked="" type="checkbox"/>
HTTP TLV Caching	<input checked="" type="checkbox"/>
DHCP TLV Caching	<input checked="" type="checkbox"/>

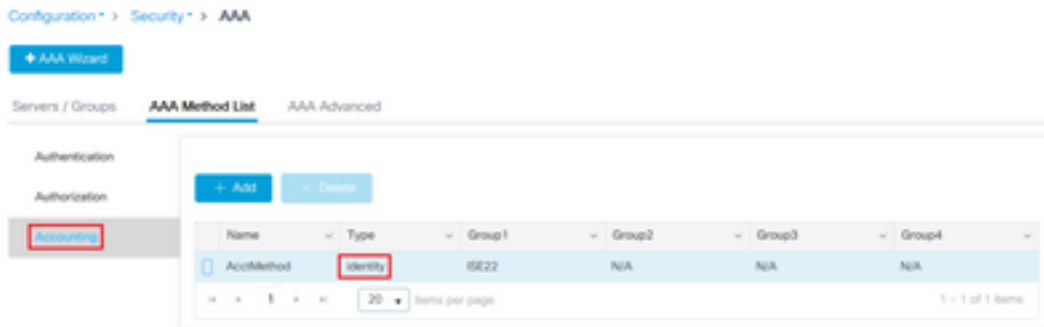
WLAN Local Profiling

Global State of Device Classification	Enabled ⓘ
Local Subscriber Policy Name	<input type="text" value="BlockPolicy"/>

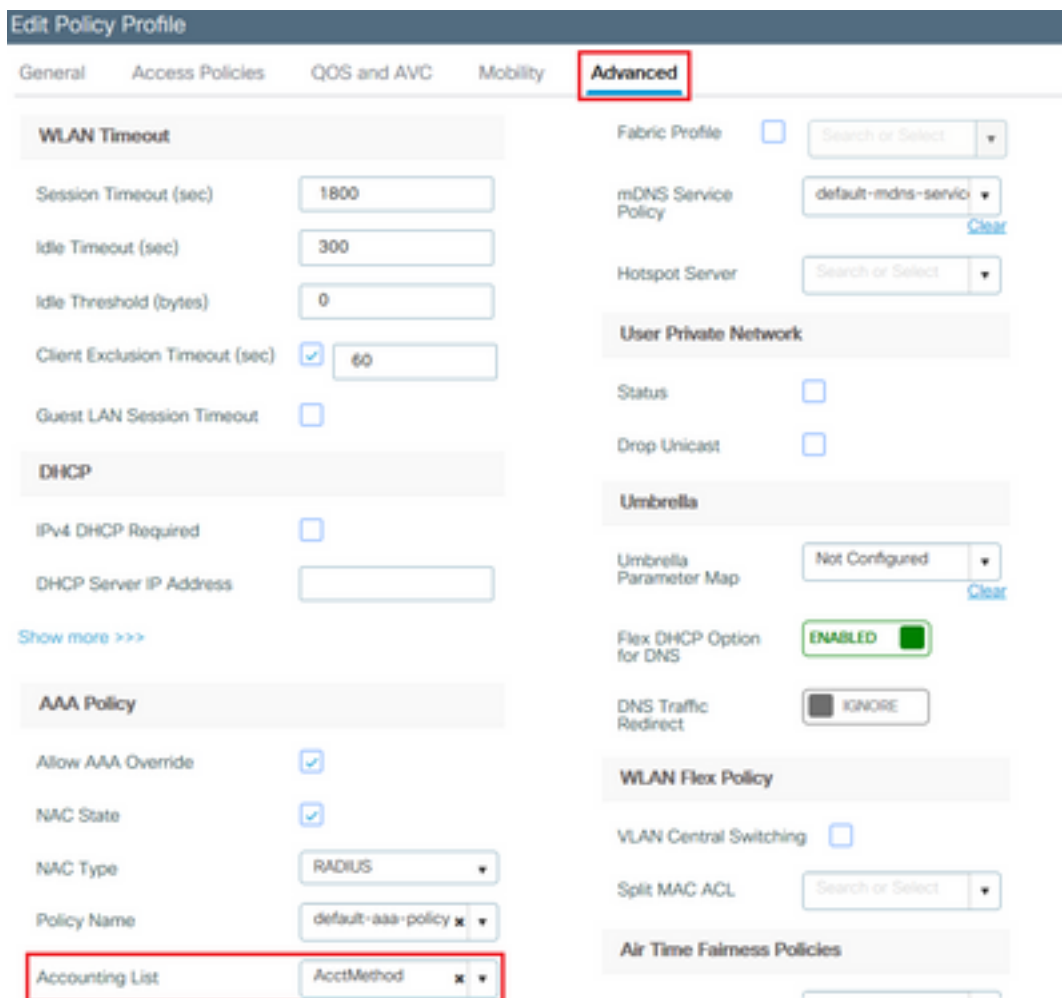
RADIUS分析配置

為了使RADIUS分析工作，除了全域性啟用裝置分類（如本地分析配置中所述），還必須：

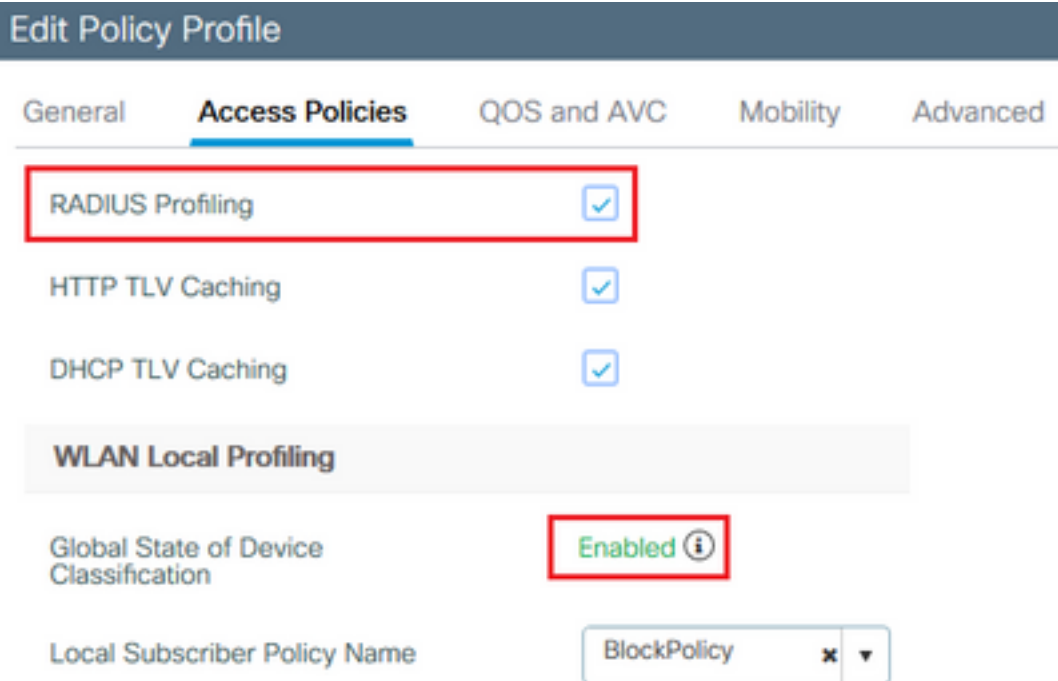
1.使用指向RADIUS伺服器的「標識」型別配置AAA記帳方法：



2.需要在Configuration > Tags & Profiles > Policy > [Policy_Name] > Advanced下新增記帳方法：



3.最後，需要在Configuration > Tags & Profiles > Policy下勾選RADIUS Profiling覈取方塊。此覈取方塊啟用HTTP和DHCP RADIUS分析（舊的AireOS WLC有兩個單獨的覈取方塊）：



分析使用案例

基於區域性特徵分類的應用區域性策略

此示例配置演示了具有QoS配置檔案阻止Youtube和facebook訪問的本地策略的配置，該配置僅適用於被描述為Windows-Workstation的裝置。

稍作更改後，可以修改此配置，例如，為僅無線電話設定特定的DSCP標籤。

導航到**Configuration > Services > QoS**以建立QoS配置檔案。按一下「新增」以建立新策略：



指定策略名稱並新增新類對映。從可用協定中，選擇需要被阻止、已標籤DSCP或頻寬受限的協定。

在這個例子中，youtube和facebook被遮蔽。請確保不要將此QoS配置檔案應用到QoS視窗底部的任何策略配置檔案：

Add QoS

Auto QoS DISABLED

Policy Name*

Description

Match Type	Match Value	Mark Type	Mark Value	Police Value (kpbs)	Drop	AVC/User Defined	Actions
No items to display							

+ Add Class-Maps - Delete

AVC/User Defined

Match Any All

Drop

Match Type

Available Protocol(s)

Selected Protocol(s)

Available (8) Selected (0)

Profiles	Ingress	Egress
<ul style="list-style-type: none"> vasa 33nps webauth 11webauth 11mobility 11override 		

導覽至Configuration > Security > Local Policy，然後建立一個新的服務模板：

Configuration > Security > Local Policy

Service Template Policy Map

+ Add - Delete

Service Template Name	Source
<input type="checkbox"/> webauth-global-inactive	
<input type="checkbox"/> DEFAULT_CRITICAL_DATA_TEMPLATE	
<input type="checkbox"/> DEFAULT_CRITICAL_VOICE_TEMPLATE	
<input type="checkbox"/> DEFAULT_LINKSEC_POLICY_MUST_SECURE	
<input type="checkbox"/> DEFAULT_LINKSEC_POLICY_SHOULD_SECURE	

1 - 5 of 5 items

指定在上一步中建立的Ingress和Egress QoS配置檔案。在此步驟中還可以應用訪問清單。如果不需要更改VLAN，請將vlan欄位留空：

✕
Create Service Template

Service Template Name*	BlockTemplate
VLAN ID	1-4094
Session Timeout (secs)	1-65535
Access Control List	None ▼
Ingress QoS	block ✕ ▼
Egress QoS	block ✕ ▼
mDNS Service Policy	Search or Select ▼

↶ Cancel

📄 Apply to Device

導航到Policy Map頁籤，然後點選add:

Configuration* > Security* > Local Policy

Service Template Policy Map

➕ Add

✖ Delete

Policy Map Name
<input type="checkbox"/> BUILTIN_AUTOCONF_POLICY

1 - 1 of 1 items

設定策略對映名稱並新增新條件。指定在上一步中建立的服務模板，並選擇應用此模板的裝置型別。

本例中使用的是Microsoft-Workstation。如果定義了多個策略，則使用第一個匹配項。

另一個常見用例是指定基於OUI的匹配條件。如果部署具有大量相同型號的掃描器或印表機，它們通常具有相同的MAC OUI。

這可用於應用特定的QoS DSCP標籤或ACL:

Create Policy Map Configuration

Policy Map Name *

Match Criteria List

+ Add - Delete Move To + Move Up + Move Down

Device Type(Match Criteria)	User Role(Match Criteria)	User Name(Match Criteria)	OUI(Match Criteria)	MAC Address(Match Criteria)	Service Template
No items to display					

20 items per page

Add Match Criteria

Service Template *

Device Type

User Role

User Name

OUI

MAC Address

為了讓WLC能夠識別youtube和facebook流量，需要開啟應用可視性。

導覽至Configuration > Services > Application Visibility e對您的WLAN的策略配置檔案進行不可見性：

Configuration > Services > Application Visibility

Enable AVC Define Policy

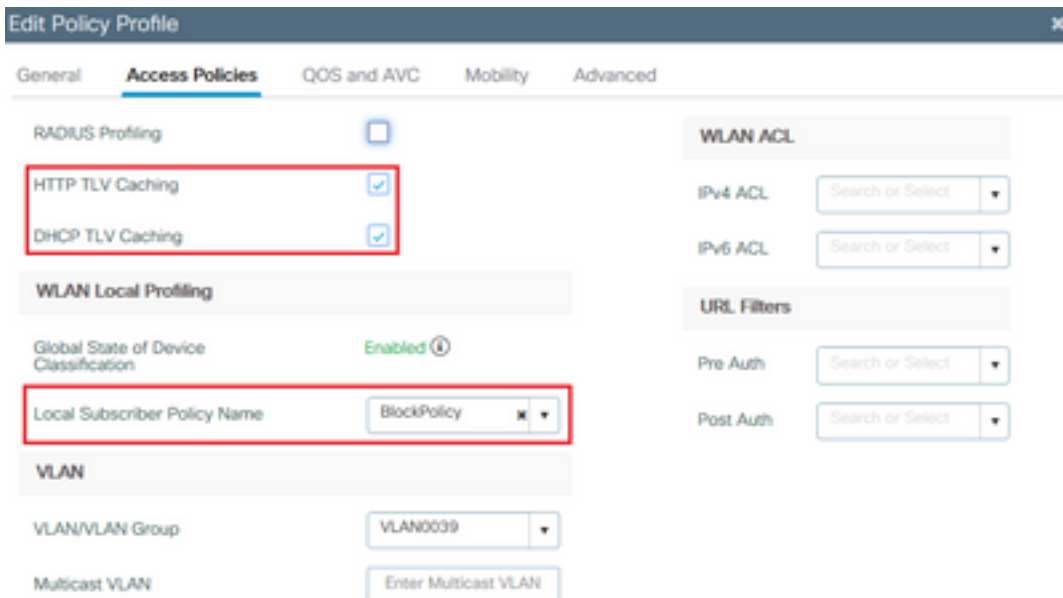
Available (11)

Profiles	Visibility	Collector Address
11feedback		
11mobility		
11profiling		
33nps		
Capwap1		
default-policy-profile		

Enabled (1)

Profiles	Visibility	Collector Address
11override	<input checked="" type="checkbox"/>	Local <input checked="" type="checkbox"/> External <input type="checkbox"/>

確認在策略Profile下啟用了HTTP TLV快取、DHCP TLV快取和全域性裝置分類，並且本地使用者策略指向在前面步驟之一建立的本地策略對映：



客戶端連線後，可以檢查是否已應用本地策略，並測試youtube和facebook是否實際被阻止。

show wireless client mac-address [MAC_ADDR] detailed的輸出包括：

```
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_lloverride_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高級策略集的RADIUS分析

啟用RADIUS分析後，WLC會將分析資訊轉發到ISE。根據此資訊，可以建立高級身份驗證和授權規則。

本文不涉及ISE配置。有關詳細資訊，請參閱[Cisco ISE分析設計手冊](#)。

此工作流程通常需要使用CoA，因此請確保在9800 WLC上啟用此工作流程。

在FlexConnect部署中進行分析

集中身份驗證、本地交換

在此設定中，「本地」和「RADIUS」分析繼續工作，與前幾章中所述的工作完全相同。如果AP進入獨立模式（AP失去與WLC的連線），裝置分析將停止工作，並且沒有新的客戶端能夠連線。

本地身份驗證、本地交換

如果AP處於連線模式（AP加入到WLC），分析將繼續工作（AP將客戶端DHCP資料包的副本傳送到WLC以執行分析過程）。

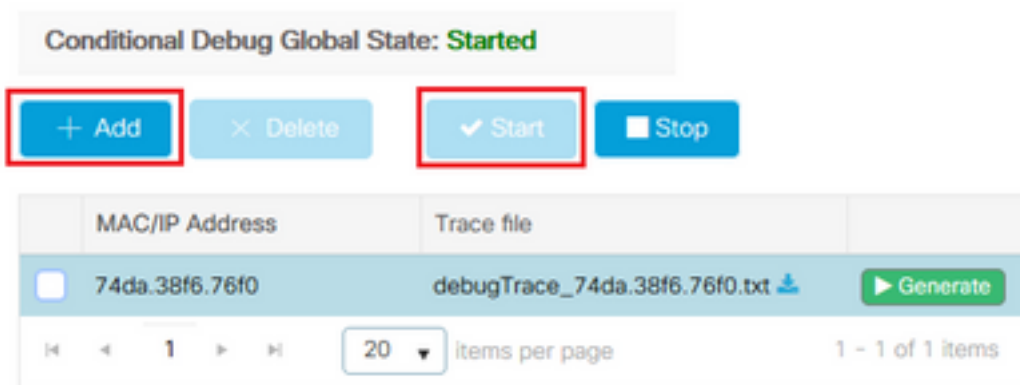
儘管分析工作正常，但由於身份驗證是在AP本地執行的，因此不能將分析資訊用於任何本地策略配置或RADIUS分析規則。

疑難排解

放射性痕跡

對WLC上的客戶端配置進行故障排除的最簡單方法是使用放射性跟蹤。導覽至Troubleshooting > Radiative Trace，輸入使用者端無線配接器MAC位址，然後按一下「Start:

Troubleshooting > Radioactive Trace



The screenshot shows the 'Radioactive Trace' interface. At the top, it indicates 'Conditional Debug Global State: Started'. Below this are four buttons: '+ Add', '× Delete', '✓ Start', and '■ Stop'. The 'Start' button is highlighted with a red box. Below the buttons is a table with two columns: 'MAC/IP Address' and 'Trace file'. The table contains one entry with the MAC address '74da.38f6.76f0' and the trace file 'debugTrace_74da.38f6.76f0.txt'. A 'Generate' button is next to the trace file. At the bottom, there is a pagination control showing '20 items per page' and '1 - 1 of 1 items'.

將客戶端連線到網路，並等待其進入運行狀態。停止跟蹤並按一下**Generate**。確保啟用內部日誌（此選項僅存在於17.1.1及更高版本中）：

Enter time interval
✕

Enable Internal Logs

Generate logs for last

10 minutes

30 minutes

1 hour

since last boot

0-4294967295

seconds ▼

↶ Cancel

📄
Apply to Device

放射性痕跡的相關片段可在下面找到：

WLC將使用者端設定為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快取裝置分類：

```

(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在快取中查詢裝置分類：

```

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

```

WLC應用基於分類的本地策略：

```

(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傳送包含DHCP和HTTP分析屬性的記帳資料包：


```

[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

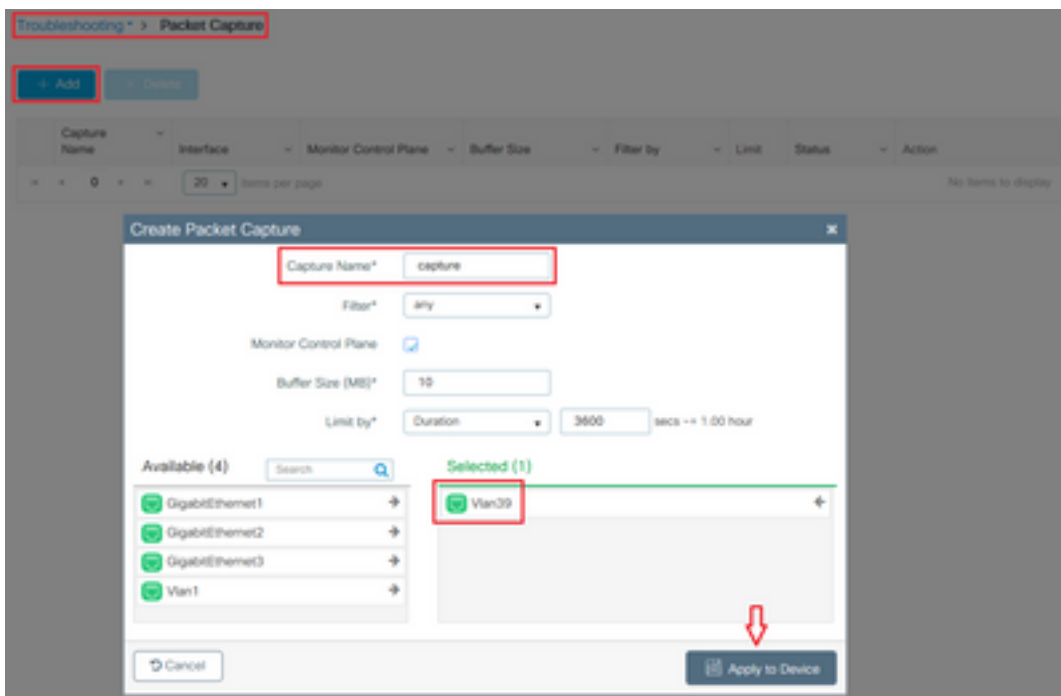
### http profiling sent in a separate accounting packet
[aaa-attr-inf] [21168]: (debug): Get acct attrs http-tlv 0 00 01 00 0e 4d 69 63 72 6f 73 6f 66
74 20 4e 43 53 49

```

封包擷取

在集中交換部署中，可以在WLC本身上執行封包擷取。導覽至Troubleshooting > Packet Capture，並在此客戶端正在使用的其中一個介面上建立新的捕獲點。

必須在vlan上安裝SVI，才能在其上執行捕獲，否則要在物理埠上執行捕獲



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。