

# 9800 Wireless LAN Controller에서 클라이언트 프로파일링 시연

## 목차

### [소개](#)

[사용되는 구성 요소](#)

[프로파일링 프로세스](#)

[MAC 주소 OUI 프로파일링](#)

[로컬로 관리되는 MAC 주소 문제](#)

[DHCP 프로파일링](#)

[HTTP 프로파일링](#)

[RADIUS 프로파일링](#)

[DHCP RADIUS 프로파일링](#)

[HTTP RADIUS 프로파일링](#)

[9800 WLC에서 프로파일링 구성](#)

[로컬 프로파일링 컨피그레이션](#)

[RADIUS 프로파일링 컨피그레이션](#)

[활용 사례 프로파일링](#)

[로컬 프로파일링 분류를 기반으로 로컬 정책 적용](#)

[Cisco ISE의 고급 정책 집합에 대한 RADIUS 프로파일링](#)

[FlexConnect 구축에서 프로파일링](#)

[중앙 인증, 로컬 스위칭](#)

[로컬 인증, 로컬 스위칭](#)

[문제 해결](#)

[방사선 흔적](#)

[패킷 캡처](#)

## 소개

이 문서에서는 Cisco Catalyst 9800 Wireless LAN Controller에서 장치 분류 및 프로파일링이 작동하는 방법을 설명합니다.

## 사용되는 구성 요소

- 17.2.1 이미지를 실행하는 9800 CL WLC
- 1815i 액세스 포인트
- Windows 10 Pro 무선 클라이언트
- Cisco ISE 2.7

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 프로파일링 프로세스

이 문서에서는 Cisco Catalyst 9800 Wireless LAN Controller에서 장치 분류 및 프로파일링이 작동하는 방식을 심층적으로 살펴보고 잠재적인 사용 사례, 구성 예 및 문제 해결에 필요한 단계를 설명합니다.

장치 프로파일링은 무선 인프라에 연결된 무선 클라이언트에 대한 추가 정보를 찾을 수 있는 방법을 제공하는 기능입니다.

장치 프로파일링이 수행되면 다른 로컬 정책을 적용하거나 특정 RADIUS 서버 규칙을 확인하는 데 사용할 수 있습니다.

Cisco 9800 WLC는 세 가지 유형의 디바이스 프로파일링을 수행할 수 있습니다.

1. MAC 주소 OUI
2. DHCP
3. HTTP

## MAC 주소 OUI 프로파일링

MAC 주소는 각 무선(및 유선) 네트워크 인터페이스의 고유한 식별자입니다. 일반적으로 16진수 형식 MM:MM:MM:SS:SS로 기록되는 48비트 숫자입니다.

처음 24비트(또는 3옥텟)는 OUI(Organizationally Unique Identifier)라고 하며 공급업체나 제조업체를 고유하게 식별합니다.

IEEE에서 구매하고 할당합니다. 한 공급업체 또는 제조업체에서 여러 OUI를 구매할 수 있습니다.

예:

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

무선 클라이언트가 액세스 포인트에 연결되면 WLC는 OUI 조회를 수행하여 제조업체를 확인합니다.

Flexconnect 로컬 스위칭 구축에서 AP는 여전히 관련 클라이언트 정보를 WLC에 릴레이합니다(예: DHCP 패킷 및 클라이언트 mac 주소).

OUI만을 기반으로 하는 프로파일링은 극히 제한적이며, 특정 브랜드로 기기를 분류할 수는 있으나, 노트북과 스마트폰을 구분할 수는 없다.

## 로컬로 관리되는 MAC 주소 문제

개인 정보 보호 문제로 인해 많은 제조업체가 mac 임의 지정 기능을 장치에 구현하기 시작했습니다.

로컬로 관리되는 MAC 주소는 무작위로 생성되고, 주소의 첫 번째 옥텟의 두 번째 최하위 비트가 1로 설정된다.

이 비트는 mac 주소가 실제로 무작위로 생성된 주소임을 알리는 플래그 역할을 합니다.

로컬로 관리되는 MAC 주소의 네 가지 가능한 형식이 있습니다(x는 16진수 값일 수 있음).

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

기본적으로 Android 10 디바이스는 새 SSID 네트워크에 연결할 때마다 무작위로 생성된 로컬로 관리되는 MAC 주소를 사용합니다.

컨트롤러가 주소가 임의 지정되었음을 인식하고 조회를 수행하지 않으므로 이 기능은 OUI 기반 디바이스 분류를 완전히 무효화합니다.

## DHCP 프로파일링

무선 클라이언트가 전송 중인 DHCP 패킷을 조사하여 WLC에서 DHCP 프로파일링을 수행합니다.

DHCP 프로파일링을 사용하여 디바이스를 분류한 경우 **show wireless client mac-address [MAC\_ADDR]** 세부 명령의 출력에는 다음이 포함됩니다.

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

WLC는 무선 클라이언트에서 보낸 패킷의 여러 DHCP 옵션 필드를 검사합니다.

### 1. 옵션 12 - 호스트 이름

이 옵션은 클라이언트 호스트 이름을 나타내며 DHCP Discover 및 DHCP Request 패킷에서 찾을 수 있습니다.

| 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: 000000000000000000000000
  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-KL8E0M4
```

### 2. 옵션 60 - 공급업체 클래스 식별자

이 옵션은 DHCP Discover 및 Request 패킷에도 있습니다.

이 옵션을 사용하면 클라이언트가 DHCP 서버에 대해 자신을 식별할 수 있으며, 특정 공급업체 클래스 식별자를 가진 클라이언트에만 응답하도록 서버를 구성할 수 있습니다.

이 옵션은 네트워크에서 액세스 포인트를 식별하고 옵션 43을 통해서만 응답하는 데 가장 일반적으로

로 사용됩니다.

공급업체 클래스 식별자 예

- "MSFT 5.0" 모든 Windows 2000 클라이언트(이상)
- "MSFT 98" 모든 Windows 98 및 Me 클라이언트
- "MSFT" 모든 Windows 98, Me 및 2000 클라이언트

Apple MacBook 디바이스는 기본적으로 옵션 60을 전송하지 않습니다.

Windows 10 클라이언트의 패킷 캡처 예:

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

### 3. 옵션 55 - 매개변수 요청 목록

DHCP Parameter Request List(DHCP 매개변수 요청 목록) 옵션에는 DHCP 클라이언트가 DHCP 서버에서 요청하는 컨피그레이션 매개변수(옵션 코드)가 포함되어 있습니다. 심볼로 구분된 표기법(예: 1,15,43)으로 작성된 문자열입니다.

이 솔루션은 벤더에 따라 다르며 여러 디바이스 유형별로 중복될 수 있기 때문에 완벽한 솔루션은 아닙니다.

예를 들어 Windows 10 디바이스는 항상 기본적으로 특정 매개 변수 목록을 요청합니다. Apple iPhone과 iPad는 서로 다른 매개변수 집합을 사용하므로 이를 분류할 수 있습니다.

Windows 10 클라이언트의 캡처 예:

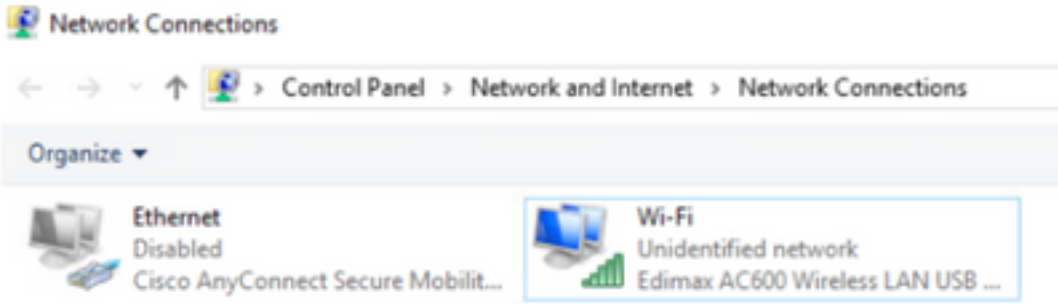
```
Option: (55) Parameter Request List
Length: 14
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter 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. 옵션 77 - 사용자 클래스

사용자 클래스는 기본적으로 사용되지 않는 옵션이며 클라이언트를 수동으로 구성해야 합니다. 예를 들어 다음 명령을 사용하여 Windows 시스템에서 이 옵션을 구성할 수 있습니다.

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

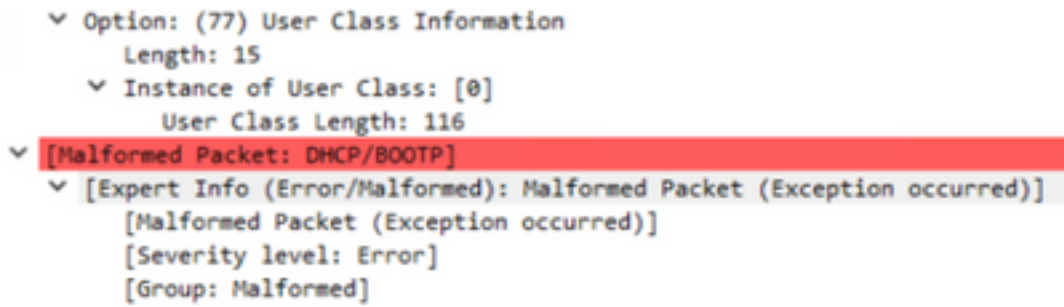
어댑터 이름은 제어판의 네트워크 및 공유 센터에서 찾을 수 있습니다.



CMD에서 Windows 10 클라이언트용 DHCP 옵션 66을 구성합니다(관리자 권한 필요).

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

Windows의 옵션 66 구현으로 인해 wireshark는 이 옵션을 디코딩할 수 없으며, 옵션 66 이후에 오는 패킷의 일부가 잘못된 형식으로 표시됩니다.



## HTTP 프로파일링

HTTP 프로파일링은 9800 WLC가 지원하는 프로파일링의 가장 고급 방법이며 가장 세부적인 장치 분류를 제공합니다.

클라이언트가 HTTP 프로파일링되려면 "Run" 상태여야 하며 HTTP GET 요청을 수행해야 합니다.

WLC는 요청을 가로채고 패킷의 HTTP 헤더에서 "User-Agent" 필드를 검사합니다.

이 필드에는 분류하는 데 사용할 수 있는 무선 클라이언트에 대한 추가 정보가 포함되어 있습니다.

기본적으로 거의 모든 제조업체는 무선 클라이언트가 인터넷 연결 확인을 시도하는 기능을 구현했습니다.

이 검사는 자동 게스트 포털 탐지에 사용됩니다. 디바이스가 상태 코드 200(OK)을 사용하여 HTTP 응답을 수신하는 경우 이는 WLAN이 webauth로 보호되지 않음을 의미합니다.

그렇다면, WLC는 나머지 인증을 수행하기 위해 필요한 인터셉션을 수행한다. 이 초기 HTTP GET은 WLC가 디바이스를 프로파일링하는 데 사용할 수 있는 유일한 WLC가 아닙니다.

모든 후속 HTTP 요청은 WLC에 의해 검사되며 더욱 자세한 분류가 필요할 수 있습니다.

Windows 10 디바이스는 [msftconnecttest.com](http://msftconnecttest.com) 도메인을 사용하여 이 테스트를 수행합니다. Apple 디바이스에서는 [captive.apple.com](http://captive.apple.com)을 사용하지만, Android 디바이스에서는 일반적으로 [connectivitycheck.gstatic.com](http://connectivitycheck.gstatic.com)을 사용합니다.

이 검사를 수행하는 Windows 10 클라이언트의 패킷 캡처를 아래에서 찾을 수 있습니다. User Agent(사용자 에이전트) 필드가 **Microsoft NCSI**로 채워지면 클라이언트가 WLC에서 **Microsoft Workstation**으로 프로파일링됩니다.

```

No.    Time           Source            Destination       Protocol  Length  Info
-----
32    11.230352      10.48.39.235     64.182.6.247     DNS      83      Standard query 0x6d68 AAAA www.msftconnecttest.com
48    11.344857      64.182.6.247    10.48.39.235     DNS      249     Standard query response 0x6d68 A www.msftconnecttest.com CNAME vnc0
55    11.354877      10.48.39.235     13.187.4.52      HTTP     365     GET /connecttest.txt HTTP/1.1
79    11.379809      13.187.4.52     10.48.39.235     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_{95A00002-0B27-4F05-891B-96A84E083A48}, id 0
> Ethernet II, Src: EdimaxTe_f6:76:f0 (74:da:38:f6:76:f0), Dst: Cisco_39:41:e1 (24:7e:12:19:41:e1)
> Internet Protocol Version 4, Src: 10.48.39.235, Dst: 13.187.4.52
> Transmission Control Protocol, Src Port: 56815, Dst Port: 80, Seq: 1, Ack: 1, Len: 333
< 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 NCSI/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 79]
  
```

HTTP를 통해 프로파일링된 클라이언트에 대한 **show wireless client mac-address [MAC\_ADDR]**의 출력 예:

```

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 프로파일링

디바이스를 분류하는 데 사용되는 방법에는 로컬 및 RADIUS 프로파일링 간에 차이가 없습니다.

Radius 프로파일링이 활성화된 경우 WLC는 특정 벤더별 RADIUS 특성 집합을 통해 디바이스에 대해 학습한 정보를 RADIUS 서버에 전달합니다.

## DHCP RADIUS 프로파일링

DHCP 프로파일링을 통해 얻은 정보는 벤더별 RADIUS AVPair로 어카운팅 요청 내의 RADIUS 서버로 전송됩니다 **cisco-av-pair: dhcp-option=<DHCP option>**

WLC에서 RADIUS 서버로 각각 전송된 DHCP 옵션 12, 60 및 55에 대한 AVPairs를 표시하는 계정 관리 요청 패킷의 예(옵션 55 값은 Wireshark 디코딩으로 인해 손상된 것으로 나타날 수 있음):

| No. | Time     | Source       | Destination  | Protocol | Length | Source Port | Destination Port | Info   |
|-----|----------|--------------|--------------|----------|--------|-------------|------------------|--|
| 829 | 9.183998 | 18.48.39.212 | 18.48.71.92  | RADIUS   | 783    | 64189       | 1813             | Accounting-Request id=282                      |
| 849 | 9.188995 | 18.48.71.92  | 18.48.39.212 | RADIUS   | 62     | 1813        | 64189            | Accounting-Response id=282                     |
| 850 | 9.188995 | 18.48.71.92  | 18.48.39.212 | RADIUS   | 62     | 1813        | 64189            | Accounting-Response id=282, Duplicate Response |

```

> Frame 829: 783 bytes on wire (6264 bits), 783 bytes captured (6264 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: 18.48.39.212, Dst: 18.48.71.92
> User Datagram Protocol, Src Port: 64189, Dst Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 0x0a (10)
Length: 783
Authenticator: 21c265454b70e17168582ce362576c5
[The response to this request is in frame 849]
Attribute Value Pairs
  AVP: t=Vendor-Specific(26) l=45 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=30 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=62 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=25 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
    Type: 26
    Length: 39
    Vendor ID: ciscoSystems (9)
    VSAs: t=Cisco-APPair(1) l=33 val=http-otp=0007100041705STOP-CLASIPW
  AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    Type: 26
    Length: 32
    Vendor ID: ciscoSystems (9)
    VSAs: t=Cisco-APPair(1) l=32 val=http-otp=0007100041705STOP-CLASIPW
  AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
    Type: 26
    Length: 38
    Vendor ID: ciscoSystems (9)
    VSAs: t=Cisco-APPair(1) l=32 val=http-otp=0007100041705STOP-CLASIPW

```

## HTTP RADIUS 프로파일링

HTTP 프로파일링(HTTP GET 요청 헤더의 User-Agent 필드)을 통해 얻은 정보는 판매업체별 RADIUS AVPair로 어카운팅 요청 내의 RADIUS 서버로 전송됩니다 **cisco-av-pair: http-tlv=User-Agent=<user-agent>**

초기 연결 확인 HTTP GET 패킷에는 User-Agent 필드에 많은 정보가 포함되지 않으며 "Microsoft NCSI"만 포함됩니다. 이 간단한 값을 RADIUS 서버로 전달하는 어카운팅 패킷의 예:

| No.  | Time        | Source       | Destination  | Protocol | Length | Source Port | Destination Port | Info   |
|------|-------------|--------------|--------------|----------|--------|-------------|------------------|--|
| 4847 | 1583.868996 | 18.48.39.212 | 18.48.71.92  | RADIUS   | 790    | 57397       | 1813             | Accounting-Request id=185                      |
| 4854 | 1583.875988 | 18.48.71.92  | 18.48.39.212 | RADIUS   | 62     | 1813        | 57397            | Accounting-Response id=185                     |
| 4855 | 1583.875988 | 18.48.71.92  | 18.48.39.212 | RADIUS   | 62     | 1813        | 57397            | Accounting-Response id=185, Duplicate Response |

```

User Datagram Protocol, Src Port: 57397, Dst Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 0x09 (9)
Length: 658
Authenticator: 00004b3f36c34d4b68387940124d
[The response to this request is in frame 4854]
Attribute Value Pairs
  AVP: t=Vendor-Specific(26) l=84 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=68 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=25 vnd=ciscoSystems(9)
  AVP: t=Vendor-Specific(26) l=35 vnd=ciscoSystems(9)
    Type: 26
    Length: 35
    Vendor ID: ciscoSystems (9)
    VSAs: t=Cisco-APPair(1) l=29 val=http-tlv=0007100041705STOP-CLASIPW

```

사용자가 인터넷 검색을 시작하고 몇 가지 추가 HTTP GET 요청을 만들면 이에 대한 추가 정보를 얻을 수 있습니다.

WLC는 이 클라이언트에 대한 새 사용자 에이전트 값을 탐지하면 ISE에 추가 계정 관리 패킷을 보냅니다.

이 예에서는 클라이언트가 Windows 10 64비트 및 Firefox 76을 사용 중임을 확인할 수 있습니다.

```

4744 1995.180880 18.48.39.112 18.48.71.92 RADIUS 765 57397 1813 Accounting-Request Id=186
4749 1995.111994 18.48.71.92 18.48.39.112 RADIUS 62 1813 57397 Accounting-Response Id=186
4758 1995.111994 18.48.71.92 18.48.39.112 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: 866 (186)
Length: 723
Authenticator: 4885c9d9b8eeae76d2f5837f9844f2f
[The response to this request is in frame 4763]
Attribute Value Pairs
  > AVP: t=Vendor-Specific(26) l=44 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) l=37 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) l=26 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) l=99 vnd=ciscoSystems(P)
    Type: 26
    Length: 99
    Vendor ID: ciscoSystems (9)
    > VS: t=Cisco-APPair(1) l=93 val=http-tlv=000f00100000c111a/5.8 [Windows NT 10.0; x64; rv:76.0] Gecko/20100101 Firefox/76.0


```

## 9800 WLC에서 프로파일링 구성

### 로컬 프로파일링 컨피그레이션

로컬 프로파일링이 작동하려면 Configuration(컨피그레이션) > Wireless(무선) > Wireless Global(무선 글로벌)에서 Device Classification(디바이스 분류)을 활성화하면 됩니다. 이 옵션은 MAC OUI, HTTP 및 DHCP 프로파일링을 동시에 활성화합니다.

Configuration > Wireless > Wireless Global

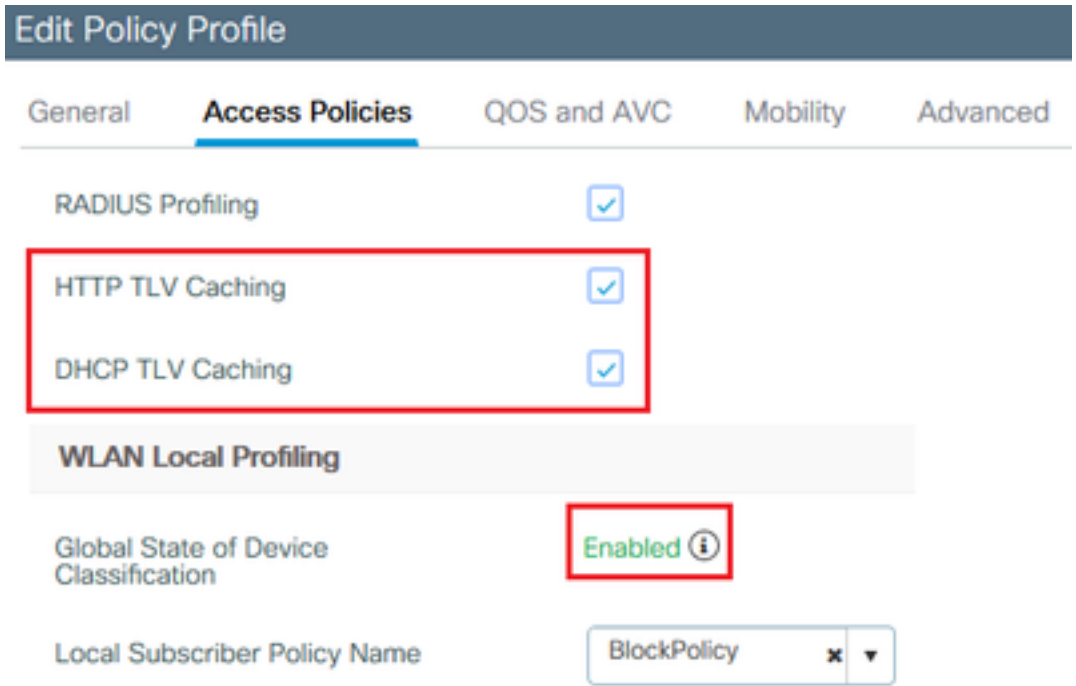
|                                  |   |
|----------------------------------|---|
| Default Mobility Domain *        | default  |
| RF Group Name*                   | default   |
| Maximum Login Sessions Per User* | 0   |
| Management Via Wireless          | <input type="checkbox"/>  |
| <b>Device Classification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

또한 Policy(정책) 컨피그레이션에서 HTTP TLV 캐싱 및 DHCP TLV 캐싱을 활성화할 수 있습니다. WLC는 프로파일링이 없어도 프로파일링을 수행합니다.

이러한 옵션이 활성화된 경우 WLC는 이전에 이 클라이언트에 대해 학습된 정보를 캐시하므로 이



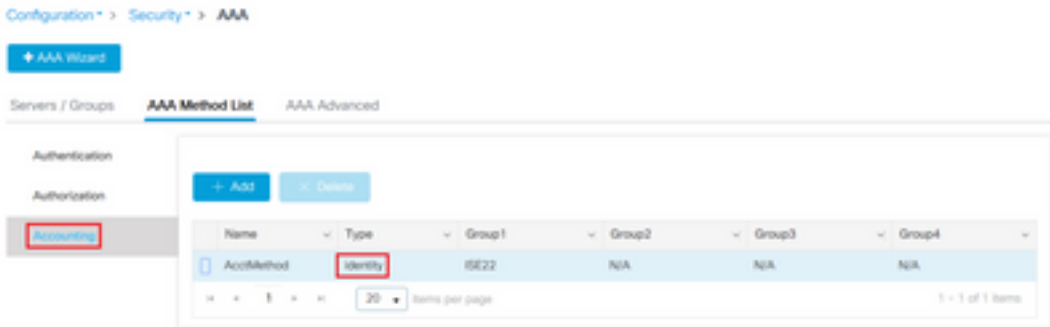
디바이스에서 생성된 추가 패킷을 검사할 필요가 없습니다.



## RADIUS 프로파일링 컨피그레이션

RADIUS 프로파일링이 작동하려면 전역적으로 디바이스 분류를 활성화하는 것(로컬 프로파일링 컨피그레이션에서 언급한 것) 외에 다음을 수행해야 합니다.

1. RADIUS 서버를 가리키는 "ID" 유형으로 AAA 계정 관리 방법을 구성합니다.



2. 회계 방법은 구성 > 태그 및 프로파일 > 정책 > [Policy\_Name] > 고급에 추가되어야 합니다.

**Edit Policy Profile**

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

---

**WLAN Timeout**

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

**AAA Policy**

Allow AAA Override

NAC State

NAC Type

Policy Name

**Accounting List**

Fabric Profile

mDNS Service Policy  [Clear](#)

Hotspot Server

**User Private Network**

Status

Drop Unicast

**Umbrella**

Umbrella Parameter Map  [Clear](#)

Flex DHCP Option for DNS  **ENABLED**

DNS Traffic Redirect

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

**Air Time Fairness Policies**

3. 마지막으로, RADIUS 프로파일링 확인란은 Configuration(구성) > Tags & Profiles(태그 및 프로필) > Policy(정책)에서 클릭해야 합니다. 이 확인란은 HTTP 및 DHCP RADIUS 프로파일링을 모두 활성화합니다(기존 AireOS WLC에는 2개의 별도 확인란이 있음).

**Edit Policy Profile**

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

---

**RADIUS Profiling**

HTTP TLV Caching

DHCP TLV Caching

**WLAN Local Profiling**

Global State of Device Classification  **Enabled** ⓘ

Local Subscriber Policy Name

**활용 사례 프로파일링**

## 로컬 프로파일링 분류를 기반으로 로컬 정책 적용

이 샘플 컨피그레이션에서는 Windows-Workstation으로 프로파일링된 디바이스에만 적용되는 Youtube 및 Facebook 액세스를 차단하는 QoS 프로필을 사용하는 로컬 정책 컨피그레이션을 보여줍니다.

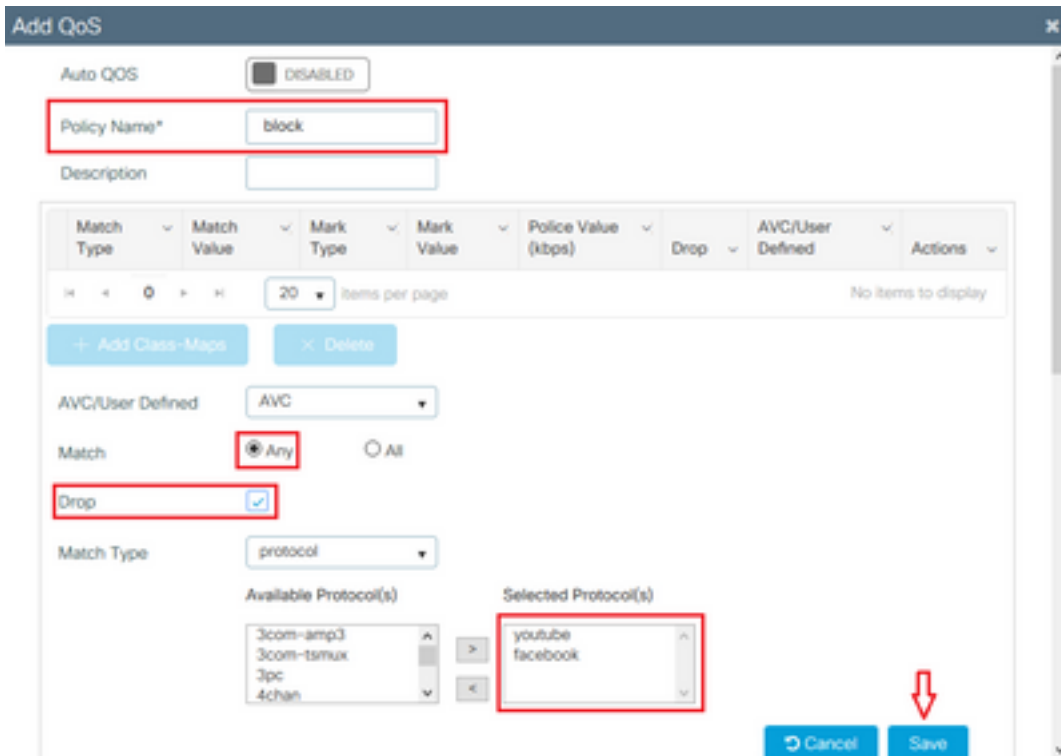
약간의 변경으로 이 컨피그레이션을 수정하여 예를 들어 무선 전화에 대해서만 특정 DSCP 마킹을 설정할 수 있습니다.

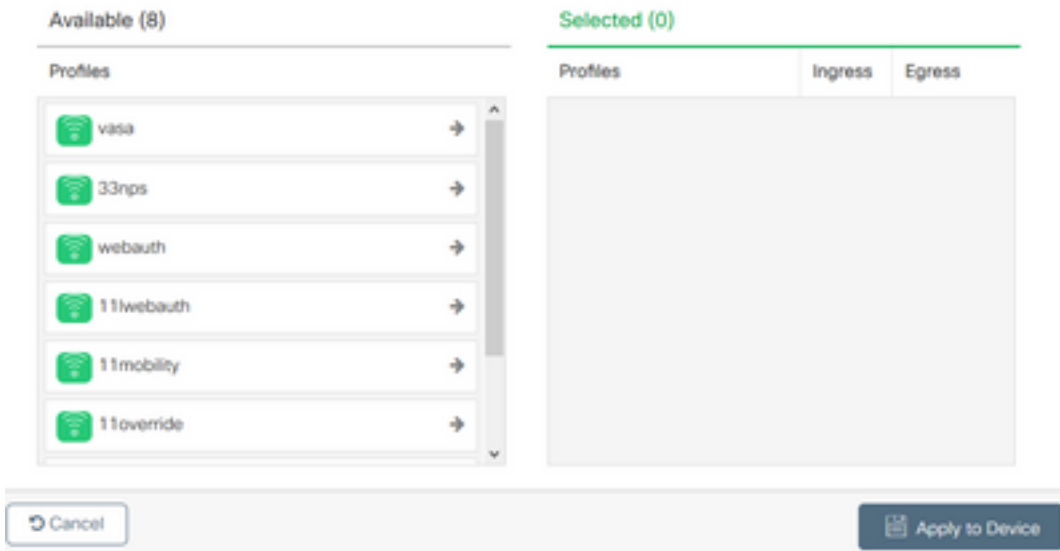
Configuration(컨피그레이션) > Services(서비스) > QoS로 이동하여 QoS 프로필을 생성합니다. Add(추가)를 클릭하여 새 정책을 생성합니다.



정책 이름을 지정하고 새 클래스 맵을 추가합니다. 사용 가능한 프로토콜에서 차단, DSCP 표시 또는 대역폭 제한이 필요한 프로토콜을 선택합니다.

이 예시에서는 youtube와 facebook이 차단됩니다. QoS 창의 하단에 있는 정책 프로필에 이 QoS 프로필을 적용하지 마십시오.

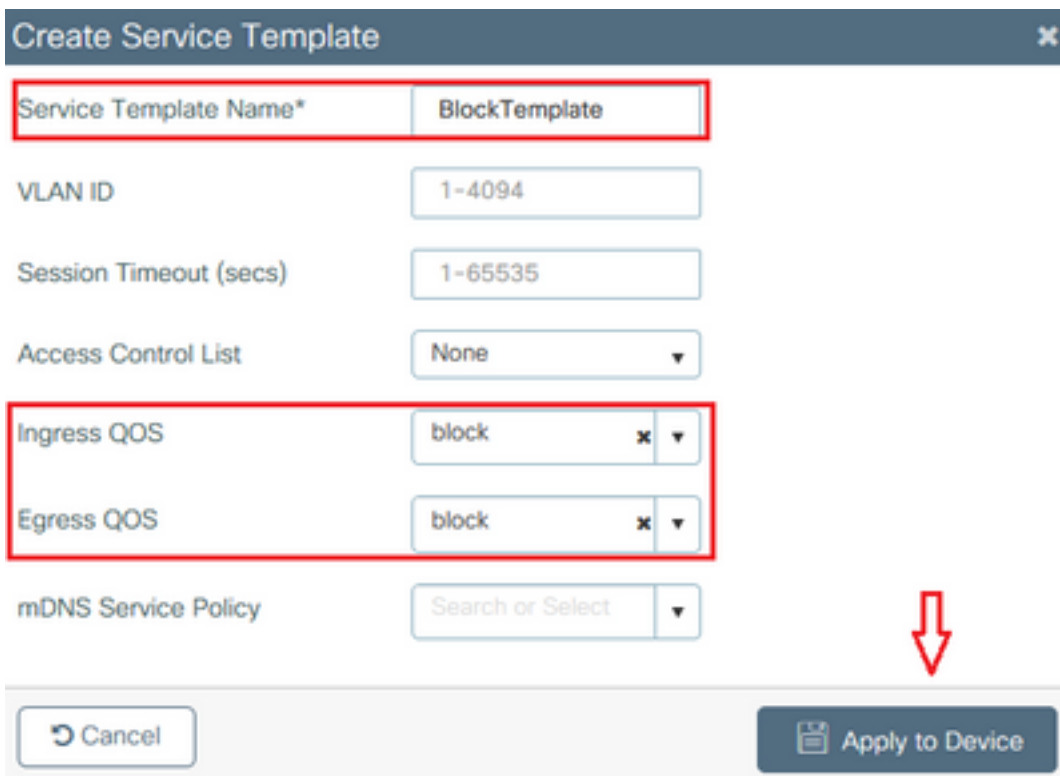




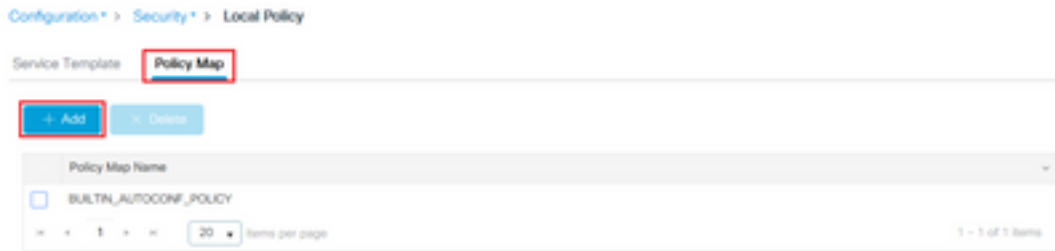
Configuration(컨피그레이션) > Security(보안) > Local Policy(로컬 정책)로 이동하여 새 서비스 템플릿을 생성합니다.



이전 단계에서 생성한 인그레스 및 이그레스 QoS 프로필을 지정합니다. 이 단계에서 액세스 목록을 적용할 수도 있습니다. VLAN을 변경할 필요가 없으면 vlan 필드를 비워둡니다.



Policy Map(정책 맵) 탭으로 이동하고 add(추가)를 클릭합니다.

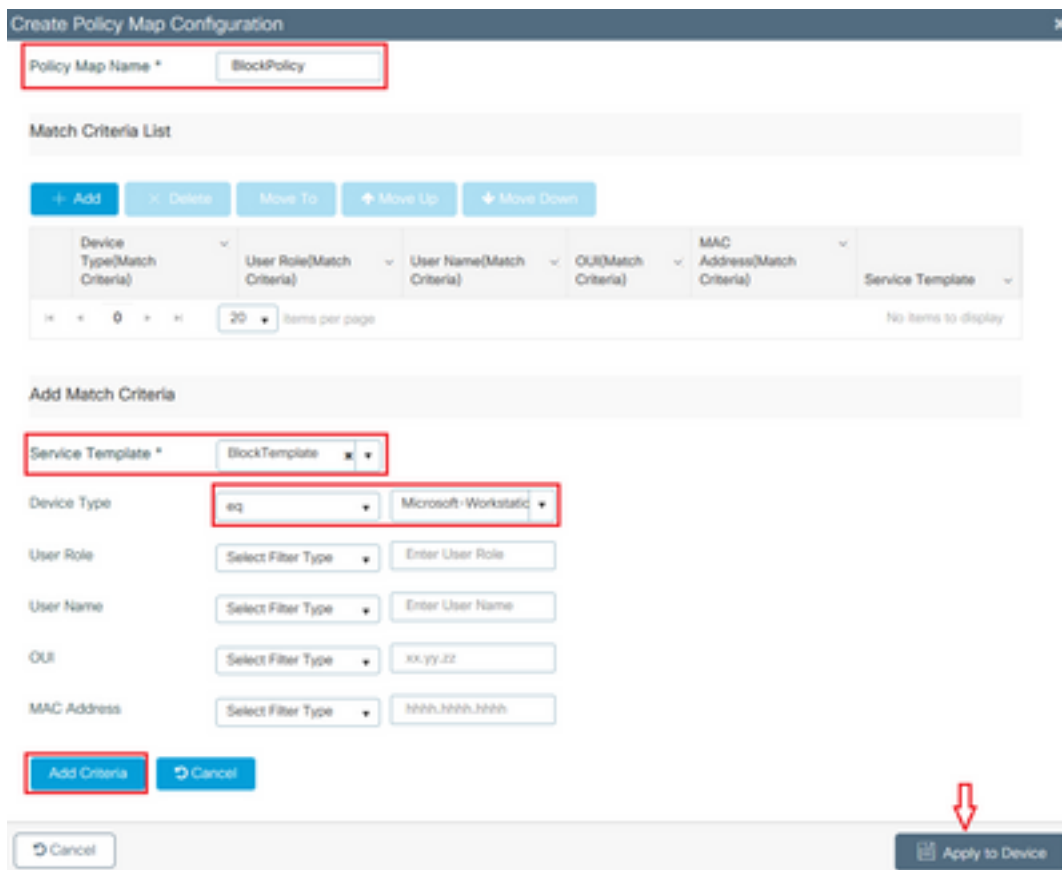


정책 맵 이름을 설정하고 새 기준을 추가합니다. 이전 단계에서 생성한 서비스 템플릿을 지정하고 이 템플릿이 적용되는 디바이스 유형을 선택합니다.

이 경우 Microsoft-Workstation이 사용됩니다. 여러 정책이 정의된 경우 첫 번째 일치기 사용됩니다.

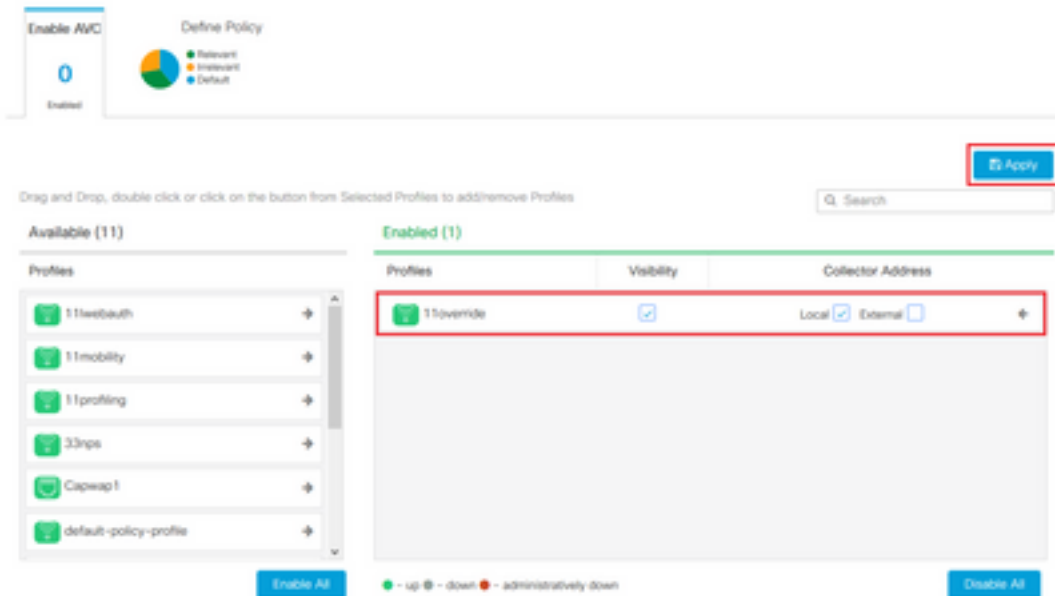
또 다른 일반적인 활용 사례는 OUI 기반 일치 기준을 지정하는 것입니다. 배포에 동일한 모델의 스캐너 또는 프린터 수가 많은 경우 일반적으로 MAC OUI가 동일합니다.

이는 특정 QoS DSCP 마킹 또는 ACL을 적용하는 데 사용할 수 있습니다.

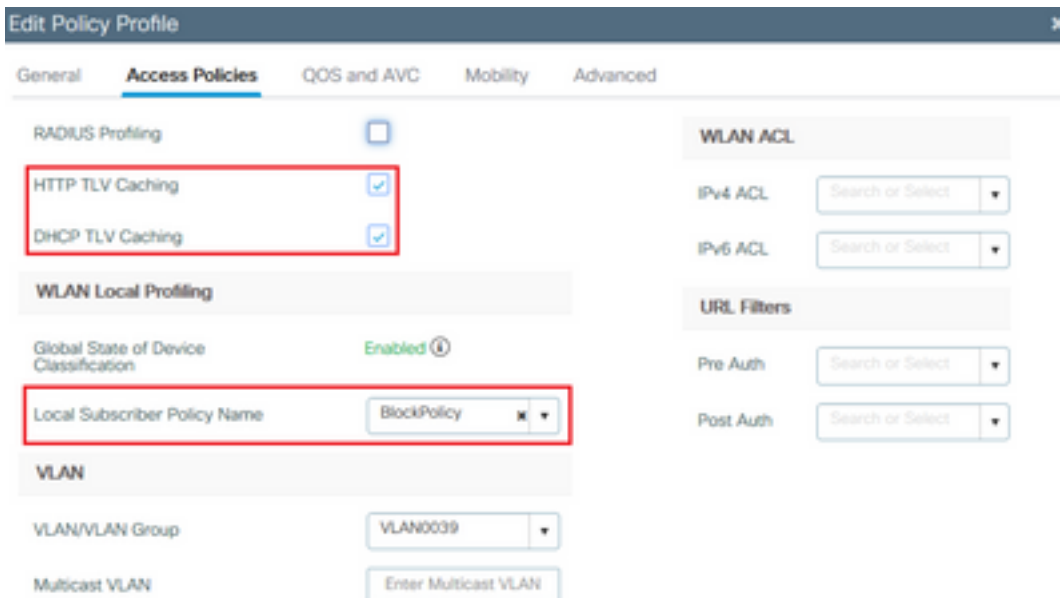


WLC가 Youtube 및 Facebook 트래픽을 인식할 수 있으려면 Application visibility(애플리케이션 가시성)를 설정해야 합니다.

Configuration(컨피그레이션) > Services(서비스) > Application Visibility(애플리케이션 가시성)로 이동합니다. WLAN의 정책 프로필에 대한 가시성 활성화:



정책 프로파일에서 HTTP TLV 캐싱, DHCP TLV 캐싱, 전역 장치 분류가 활성화되어 있고 로컬 가입자 정책이 이전 단계 중 하나에서 만든 로컬 정책 맵을 가리키고 있는지 확인합니다.



클라이언트가 연결된 후에는 현지 정책이 적용됐는지 확인하고 유튜브와 페이스북이 실제 차단됐는지 테스트할 수 있다.

show wireless client mac-address [MAC\_ADDR] 세부 정보의 출력은 다음과 같습니다.

```

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\_1loVERRIDE\_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**

## Cisco ISE의 고급 정책 집합에 대한 RADIUS 프로파일링

RADIUS 프로파일링이 활성화된 상태에서 WLC는 프로파일링 정보를 ISE에 전달합니다. 이 정보에 따라 고급 인증 및 권한 부여 규칙을 생성할 수 있습니다.

이 문서에서는 ISE 컨피그레이션을 다루지 않습니다. 자세한 내용은 [Cisco ISE 프로파일링 설계 가이드](#)를 참조하십시오.

이 워크플로는 일반적으로 CoA를 사용해야 하므로 9800 WLC에서 활성화되었는지 확인합니다.

## FlexConnect 구축에서 프로파일링

### 중앙 인증, 로컬 스위칭

이 설정에서는 로컬 및 RADIUS 프로파일링이 이전 장에서 설명한 것과 동일하게 계속 작동합니다. AP가 독립형 모드로 전환되면(AP가 WLC에 연결하지 못함) 장치 프로파일링이 작동을 중지하며 새 클라이언트가 연결할 수 없습니다.

### 로컬 인증, 로컬 스위칭

AP가 연결 모드(AP가 WLC에 조인됨)에 있으면 프로파일링이 계속 작동합니다(AP가 프로파일링 프로세스를 수행하기 위해 클라이언트 DHCP 패킷의 복사본을 WLC에 보냅니다).

프로파일링이 작동하지만 AP에서 로컬로 인증이 수행되므로 로컬 정책 컨피그레이션 또는 RADIUS 프로파일링 규칙에 대해 프로파일링 정보를 사용할 수 없습니다.

## 문제 해결

### 방사선 흔적

WLC에서 클라이언트 프로파일링 문제를 해결하는 가장 쉬운 방법은 방사능 추적을 사용하는 것입니다. Troubleshooting(트러블슈팅) > Radioactive Trace(방사능 추적)로 이동하여 클라이언트 무선 어댑터 MAC 주소를 입력하고 Start(시작):

Conditional Debug Global State: **Started**

| MAC/IP Address                          | Trace file                    |   |
|---|-------------------------------|---|
| <input type="checkbox"/> 74da.38f6.76f0 | debugTrace_74da.38f6.76f0.txt | <input type="button" value="▶ Generate"/> |

items per page
 1 - 1 of 1 items

클라이언트를 네트워크에 연결하고 실행 상태에 도달할 때까지 기다립니다. 추적을 중지하고 Generate를 클릭합니다. Internal Logs(내부 로그)가 활성화되어 있는지 확인합니다(이 옵션은 17.1.1 릴리스 이상에만 있음).

Enter time interval ×

Enable Internal Logs

Generate logs for last  10 minutes

30 minutes

1 hour

since last boot

방사능 흔적에서 관련 단편들은 아래에서 찾을 수 있다:

WLC에서 Microsoft-Workstation으로 프로파일링되는 클라이언트:

```

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
    
```



WLC에서 디바이스 분류를 캐시합니다.

```
(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
```

캐시 내에서 디바이스 분류를 찾는 WLC:

```
(info): [74da.38f6.76f0:capwap_90000004] Device type found in cache Microsoft-Workstation
분류를 기준으로 로컬 정책을 적용하는 WLC:
```

```
(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
```

DHCP 및 HTTP 프로파일링 특성을 포함하는 어카운팅 패킷을 전송하는 WLC:

```
[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
```

## 패킷 캡처

중앙 집중식 스위치드 구축에서는 WLC 자체에서 패킷 캡처를 수행할 수 있습니다.

Troubleshooting(트러블슈팅) > Packet Capture(패킷 캡처)로 이동하고 이 클라이언트에서 사용 중인 인터페이스 중 하나에 새 캡처 지점을 생성합니다.

VLAN에서 캡처를 수행하려면 SVI가 있어야 하며, 그렇지 않으면 물리적 포트 자체에서 캡처를 수행해야 합니다

Troubleshooting > Packet Capture

+ Add - Delete

| Capture Name | Interface | Monitor Control Plane | Buffer Size | Filter by | Limit | Status | Action |
|--------------|-----------|-----------------------|-------------|-----------|-------|--------|--------|
| 0            |           |                       |             |           |       |        |        |

20 items per page No items to display

### Create Packet Capture

Capture Name\* capture

Filter\* any

Monitor Control Plane

Buffer Size (MB)\* 10

Limit by\* Duration 3600 secs == 1.00 hour

Available (4)

- GgabitEthernet1
- GgabitEthernet2
- GgabitEthernet3
- Vlan1

Selected (1)

- Vlan39

Cancel Apply to Device

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.