Demuestre la definición de perfiles de clientes en el controlador LAN inalámbrico 9800

Contenido

Introducción

Este documento describe cómo funciona la clasificación y definición de perfiles de dispositivos en los controladores de LAN inalámbrica de Cisco Catalyst 9800.

Componentes Utilizados

- 9800 CL WLC que ejecuta la imagen 17.2.1
- Punto de acceso 1815i
- Cliente inalámbrico Windows 10 Pro
- Cisco ISE 2.7

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Proceso de definición de perfiles

En este artículo se ofrece un análisis en profundidad sobre cómo funcionan la clasificación y la definición de perfiles de dispositivos en los controladores de LAN inalámbrica de Cisco Catalyst 9800, se describen los posibles casos de uso, los ejemplos de configuración y los pasos necesarios para solucionar los problemas.

La creación de perfiles de dispositivos es una función que ofrece una forma de obtener información adicional sobre un cliente inalámbrico que se ha unido a la infraestructura inalámbrica.

Una vez que se realiza la creación de perfiles de dispositivos, se puede utilizar para aplicar diferentes políticas locales o para hacer coincidir reglas específicas del servidor RADIUS.

Los Cisco 9800 WLC son capaces de realizar tres (3) tipos de perfiles de dispositivos:

1. OUI de dirección MAC
2. DHCP
3. HTTP

Perfiles OUI de direcciones MAC

La dirección MAC es un identificador único de cada interfaz de red inalámbrica (y con cables). Se trata de un número de 48 bits que suele escribirse en formato hexadecimal MM:MM:MM:SS:SS:SS.

Los primeros 24 bits (o 3 octetos) se conocen como OUI (Identificador único de la organización) e identifican de forma exclusiva a un proveedor o fabricante.

Se compran a IEEE y son asignados por IEEE. Un proveedor o fabricante puede adquirir varias OUI.

Ejemplo:

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

Una vez que un cliente inalámbrico se asocia al punto de acceso, el WLC realiza la búsqueda de OUI para determinar el fabricante.

En las implementaciones de conmutación local de Flexconnect, el AP sigue transmitiendo información relevante del cliente al WLC (como paquetes DHCP y dirección MAC del cliente).

La creación de perfiles basada únicamente en OUI es extremadamente limitada y es posible clasificar el dispositivo como una marca específica, pero no puede diferenciar entre un portátil y un smartphone.

Problemas de Direcciones MAC Administradas Localmente

Debido a problemas de privacidad, muchos fabricantes comenzaron a implementar funciones de aleatorización de mac en sus dispositivos.

Las direcciones MAC administradas localmente se generan aleatoriamente y tienen un segundo

bit menos significativo del primer octeto de la dirección establecido en 1.

Este bit actúa como un indicador que anuncia que la dirección MAC es en realidad una generada aleatoriamente.

Existen cuatro formatos posibles de direcciones MAC administradas localmente (x puede ser cualquier valor hexadecimal):

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

De forma predeterminada, los dispositivos Android 10 utilizan una dirección MAC administrada localmente de forma aleatoria cada vez que se conectan a una nueva red SSID.

Esta función anula por completo la clasificación de dispositivos basada en OUI, ya que el controlador reconoce que la dirección se ha aleatorizado y no realiza ninguna búsqueda.

Perfiles DHCP

El WLC realiza la generación de perfiles DHCP a través de la investigación de los paquetes DHCP que el cliente inalámbrico está enviando.

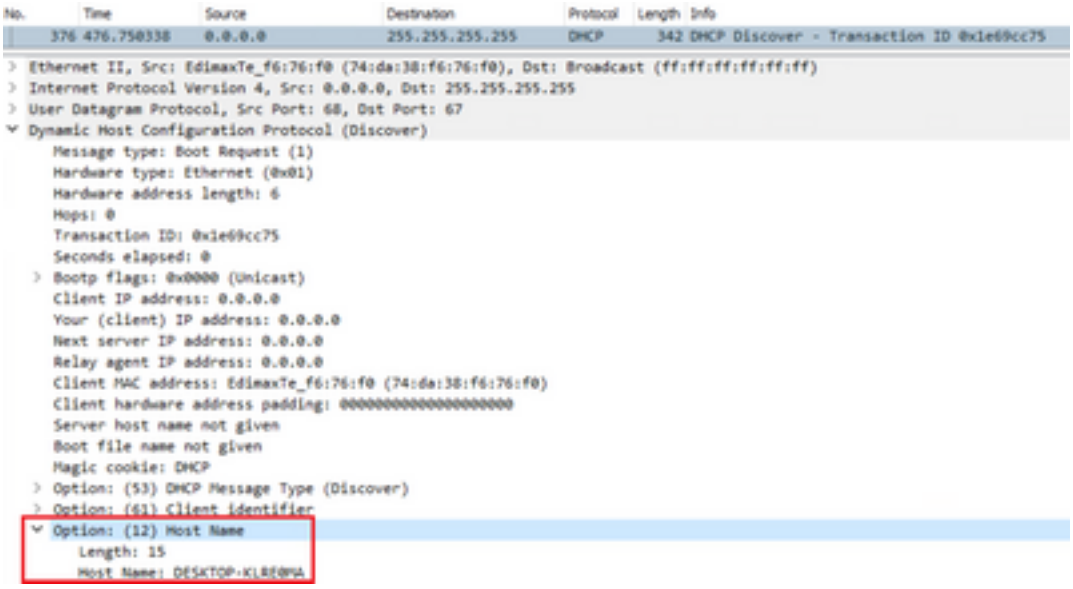
Si se utilizó la generación de perfiles DHCP para clasificar el dispositivo, el resultado del comando **show wireless client mac-address [MAC_ADDR]** detallado contiene:

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

El WLC inspecciona varios campos de la opción DHCP en los paquetes enviados por los clientes inalámbricos:

1. Opción 12: Nombre de host

Esta opción representa el nombre de host del cliente y se puede encontrar en los paquetes DHCP Discover y DHCP Request:



2. Opción 60: identificador de clase de proveedor

Esta opción también se encuentra en los paquetes DHCP Discover y Request.

Con esta opción, los clientes pueden identificarse en el servidor DHCP y los servidores se pueden configurar para responder sólo a los clientes con un identificador de clase de proveedor específico.

Esta opción se suele utilizar para identificar los puntos de acceso de la red y solo responder a ellos con la opción 43.

Ejemplos de Identificadores de Clase de Proveedor

- "MSFT 5.0" para todos los clientes de Windows 2000 (y superiores)
- "MSFT 98" para todos los clientes Windows 98 y Me
- "MSFT" para todos los clientes Windows 98, Me y 2000

Los dispositivos Apple MacBook no envían la opción 60 de forma predeterminada.

Ejemplo de captura de paquetes del cliente Windows 10:

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

3. Opción 55 - Lista de solicitudes de parámetros

La opción Lista de solicitudes de parámetros DHCP contiene parámetros de configuración (códigos de opción) que el cliente DHCP solicita al servidor DHCP. Es una cadena escrita en notación separada por comas (por ejemplo 1,15,43).

No es una solución perfecta porque los datos que produce dependen del proveedor y se pueden duplicar mediante varios tipos de dispositivos.

Por ejemplo, los dispositivos de Windows 10 siempre solicitan de forma predeterminada una lista de parámetros determinada. Los iPhones y iPads de Apple utilizan diferentes conjuntos de parámetros en los que es posible clasificarlos.

Ejemplo de captura del cliente Windows 10:

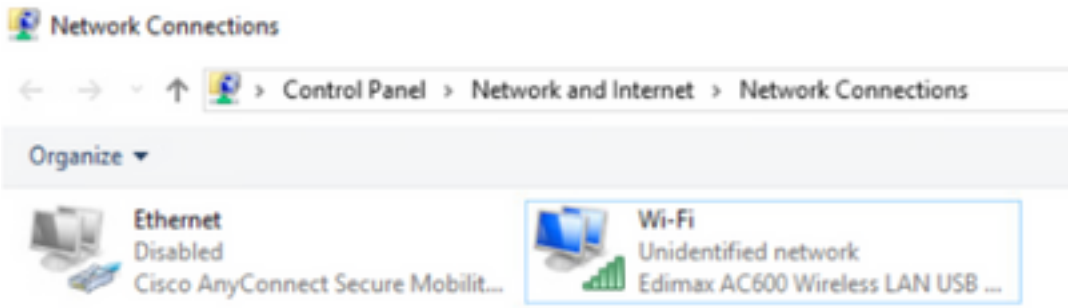
```
Option: (55) Parameter Request List
   Length: 14
   Parameter Request List Item: (1) Subnet Mask
   Parameter Request List Item: (3) Router
   Parameter Request List Item: (6) Domain Name Server
   Parameter Request List Item: (15) Domain Name
   Parameter Request List Item: (31) Perform Router 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. Opción 77 - Clase de usuario

La clase User es una opción que normalmente no se utiliza de forma predeterminada y requiere que el cliente se configure manualmente. Por ejemplo, esta opción se puede configurar en un equipo con Windows mediante el comando:

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

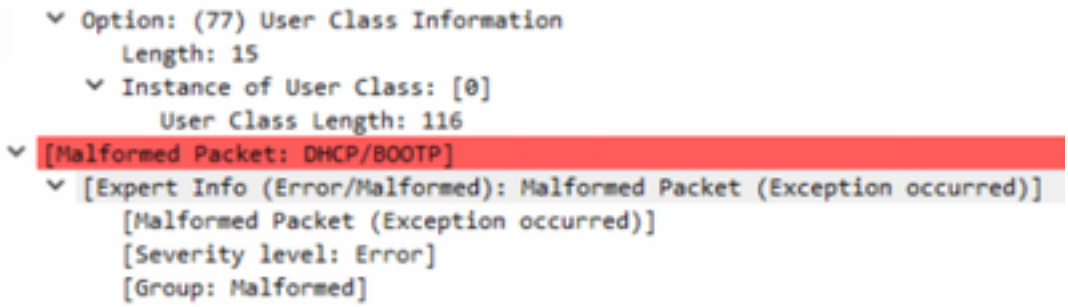
El nombre del adaptador se puede encontrar en el Centro de redes y recursos compartidos del panel de control:



Configure la opción DHCP 66 para el cliente Windows 10 en CMD (requiere derechos de administrador):

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

Windows IP Configuration

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

Debido a la implementación de Windows de la opción 66, wireshark no puede decodificar esta opción y parte del paquete que viene después de la opción 66 aparece como mal formado:



Perfiles HTTP

La definición de perfiles HTTP es la forma más avanzada de crear perfiles de compatibilidad con el WLC 9800 y ofrece la clasificación de dispositivos más detallada.

Para que un cliente tenga un perfil HTTP, debe estar en estado "Ejecutar" y realizar una solicitud GET HTTP.

El WLC intercepta la solicitud y mira en el campo "User-Agent" en el encabezado HTTP del paquete.

Este campo contiene información adicional sobre el cliente inalámbrico que se puede utilizar para clasificarlo.

De forma predeterminada, casi todos los fabricantes han implementado una función en la que un cliente inalámbrico intenta realizar una comprobación de la conectividad a Internet.

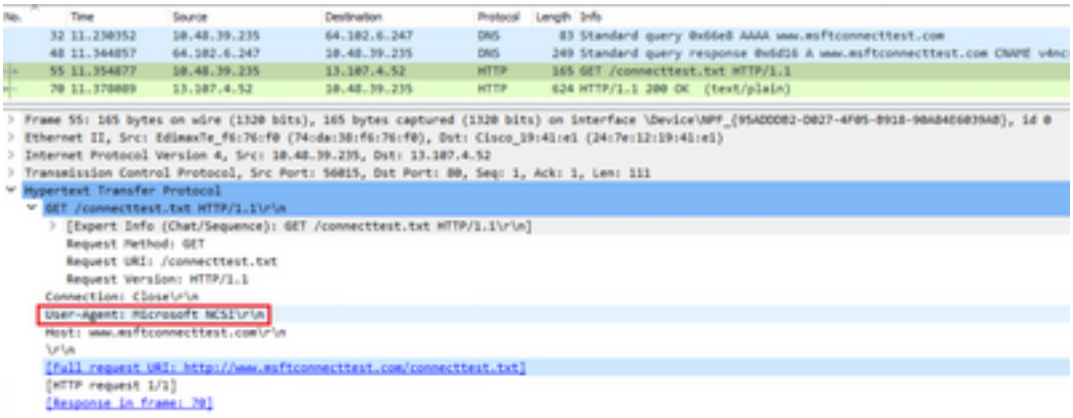
Esta comprobación también se utiliza para la detección automática del portal de invitados. Si un dispositivo recibe una respuesta HTTP con el código de estado 200 (OK), eso significa que la WLAN no está protegida con webauth.

Si es así, el WLC entonces realiza la intercepción necesaria para realizar el resto de la autenticación. Este HTTP GET inicial no es el único WLC puede utilizar para perfilar el dispositivo.

Cada solicitud HTTP subsiguiente es inspeccionada por el WLC y posiblemente resulta con una clasificación aún más detallada.

Los dispositivos Windows 10 utilizan el dominio **msftconnecttest.com** para realizar esta prueba. Los dispositivos Apple utilizan **captive.apple.com**, mientras que los dispositivos Android suelen utilizar **conntivitycheck.gstatic.com**.

Las capturas de paquetes del cliente de Windows 10 que realiza esta comprobación se pueden encontrar a continuación. El campo User Agent se llena con **Microsoft NCSI**, lo que resulta en que el cliente se perfila en el WLC como **Microsoft-Workstation**:



Ejemplo de resultado de **show wireless client mac-address [MAC_ADDR] detailed** para un cliente que se perfila a través de HTTP:

```
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
```

Perfiles RADIUS

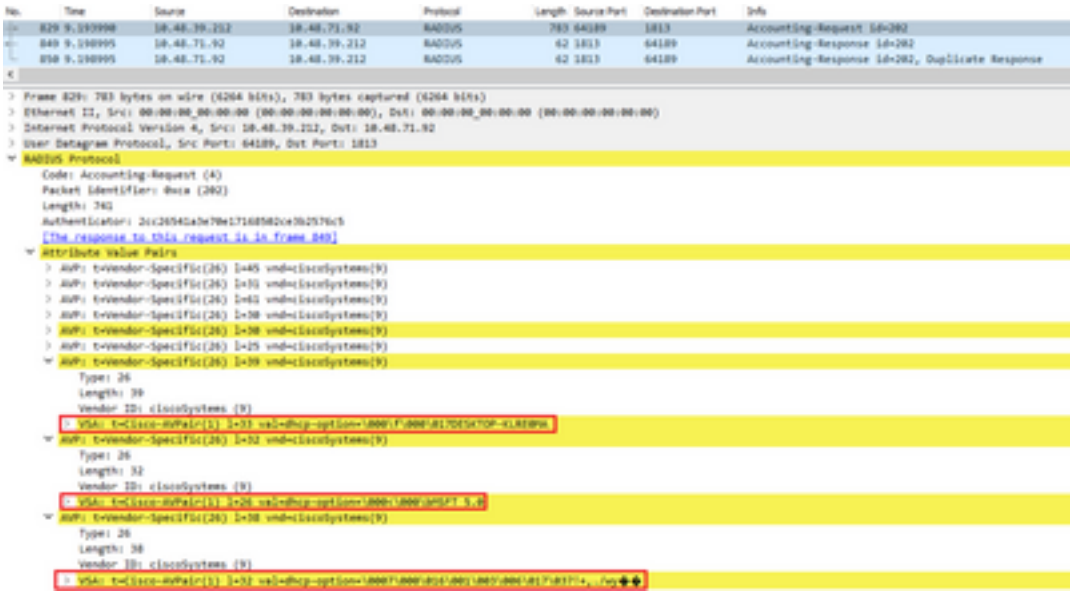
Cuando se trata de los métodos utilizados para clasificar el dispositivo, no hay diferencia entre el perfil local y el perfil RADIUS.

Si se habilita la definición de perfiles de RADIUS, el WLC reenvía la información que aprendió sobre el dispositivo a través de un conjunto específico de atributos RADIUS específicos del proveedor al servidor RADIUS.

Perfiles DHCP RADIUS

La información obtenida a través de la creación de perfiles DHCP se envía al servidor RADIUS dentro de la solicitud de contabilización como un AVPair RADIUS específico del proveedor **cisco-av-pair: dhcp-option=<opción DHCP>**

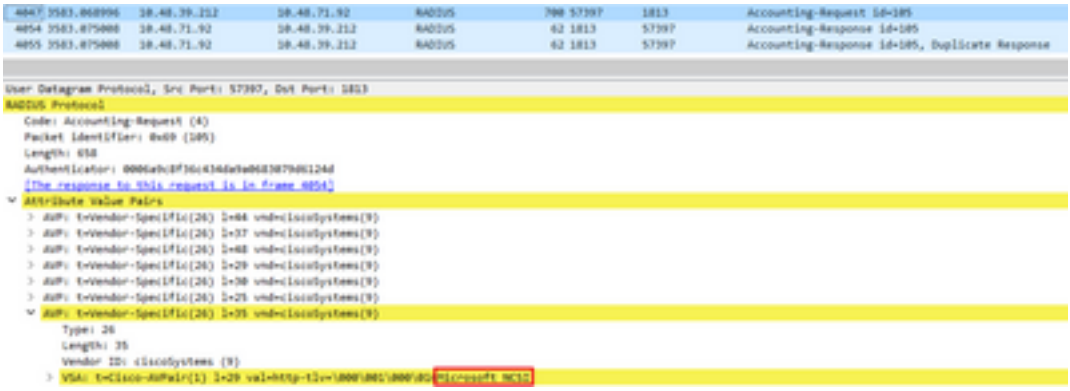
Ejemplo de un paquete de solicitud de contabilización que muestra AVPirs para la opción DHCP 12, 60 y 55, respectivamente, enviados desde el WLC al servidor RADIUS (el valor de la opción 55 posiblemente aparece como dañado debido a la decodificación de Wireshark):



Perfiles HTTP RADIUS

La información obtenida a través de perfiles HTTP (campo User-Agent del encabezado de la solicitud GET de HTTP) se envía al servidor RADIUS dentro de la solicitud de contabilización como un AVPair RADIUS específico del proveedor **cisco-av-pair: http-tlv=User-Agent=<user-agent>**

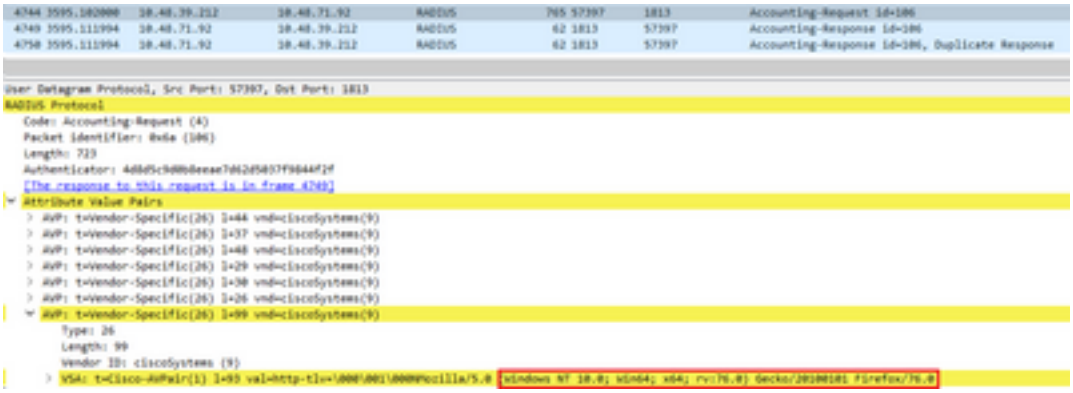
El paquete GET de HTTP de comprobación de conectividad inicial no contiene mucha información en el campo User-Agent, sólo "Microsoft NCSI". Ejemplo de un paquete de contabilización que reenvía este valor simple al servidor RADIUS:



Una vez que el usuario comienza a navegar por Internet y crea algunas solicitudes HTTP GET adicionales, es posible obtener más información sobre ello.

El WLC envía el paquete de contabilización adicional al ISE si detecta nuevos valores de agente de usuario para este cliente.

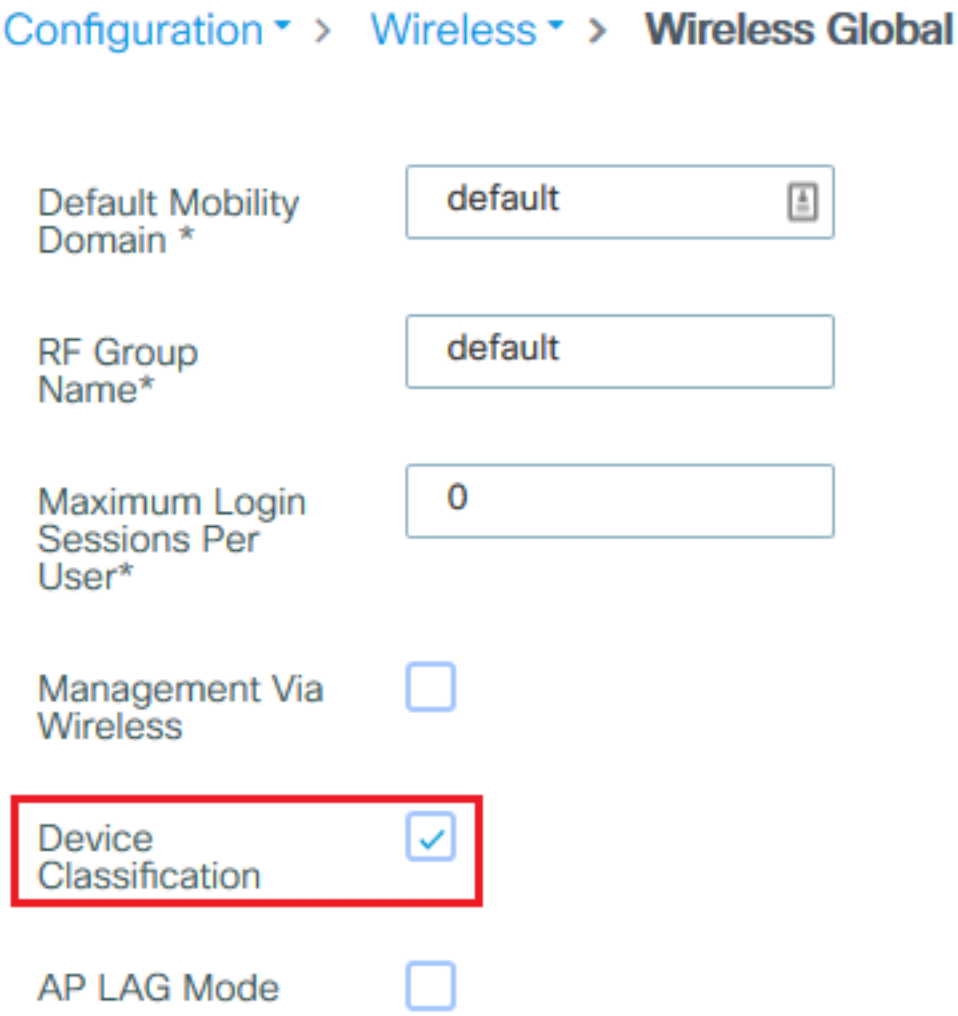
En este ejemplo, es posible ver que el cliente utiliza Windows 10 de 64 bits y Firefox 76:



Configuración de perfiles en 9800 WLC

Configuración de perfiles locales

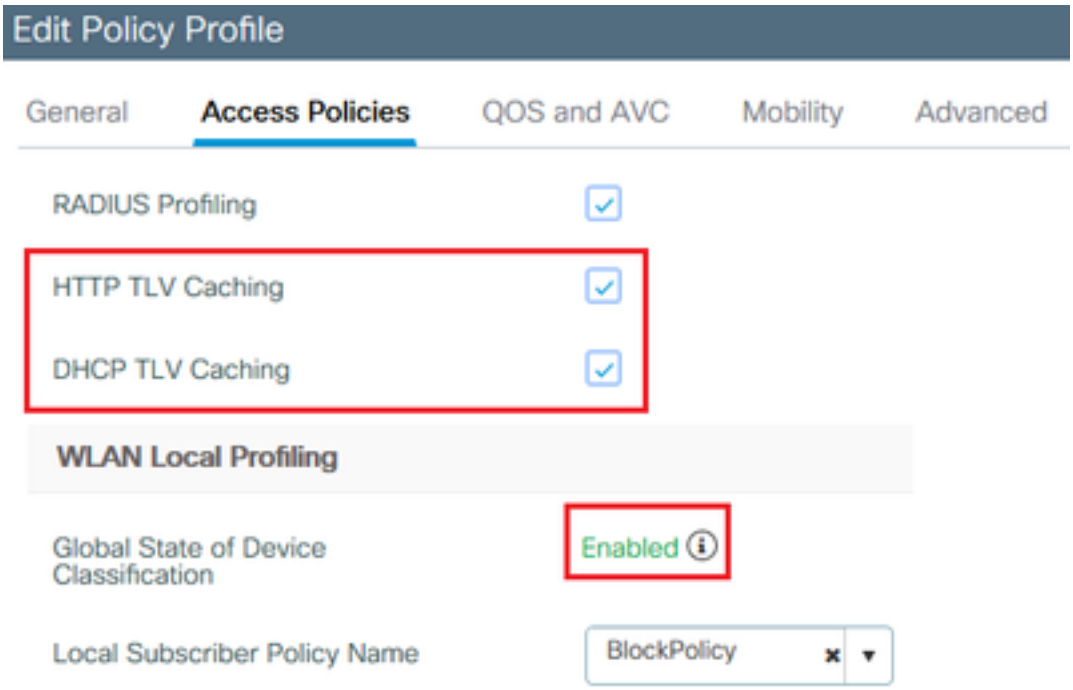
Para que la creación de perfiles local funcione, simplemente habilite Device Classification en Configuration > Wireless > Wireless Global. Esta opción permite la creación de perfiles MAC OUI, HTTP y DHCP al mismo tiempo:



Además, en Configuración de políticas puede habilitar HTTP TLV Caching y DHCP TLV Caching. El WLC realiza el perfilado incluso si sin ellos.

Con estas opciones habilitadas, el WLC luego almacena en la memoria caché información

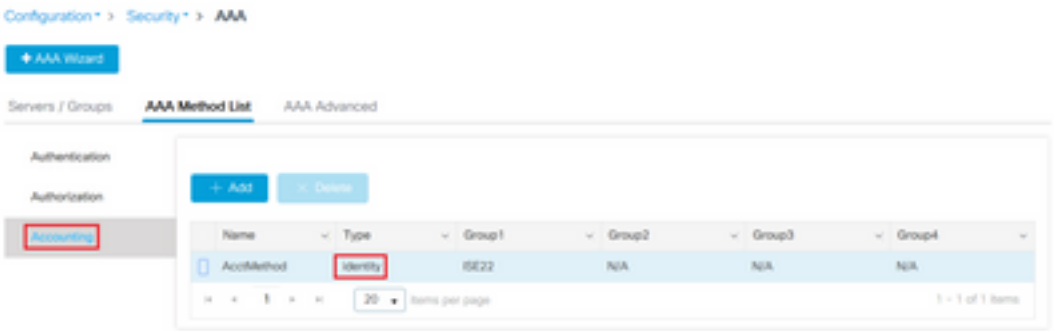
previamente aprendida sobre este cliente y evita la necesidad de inspeccionar paquetes adicionales generados por este dispositivo.



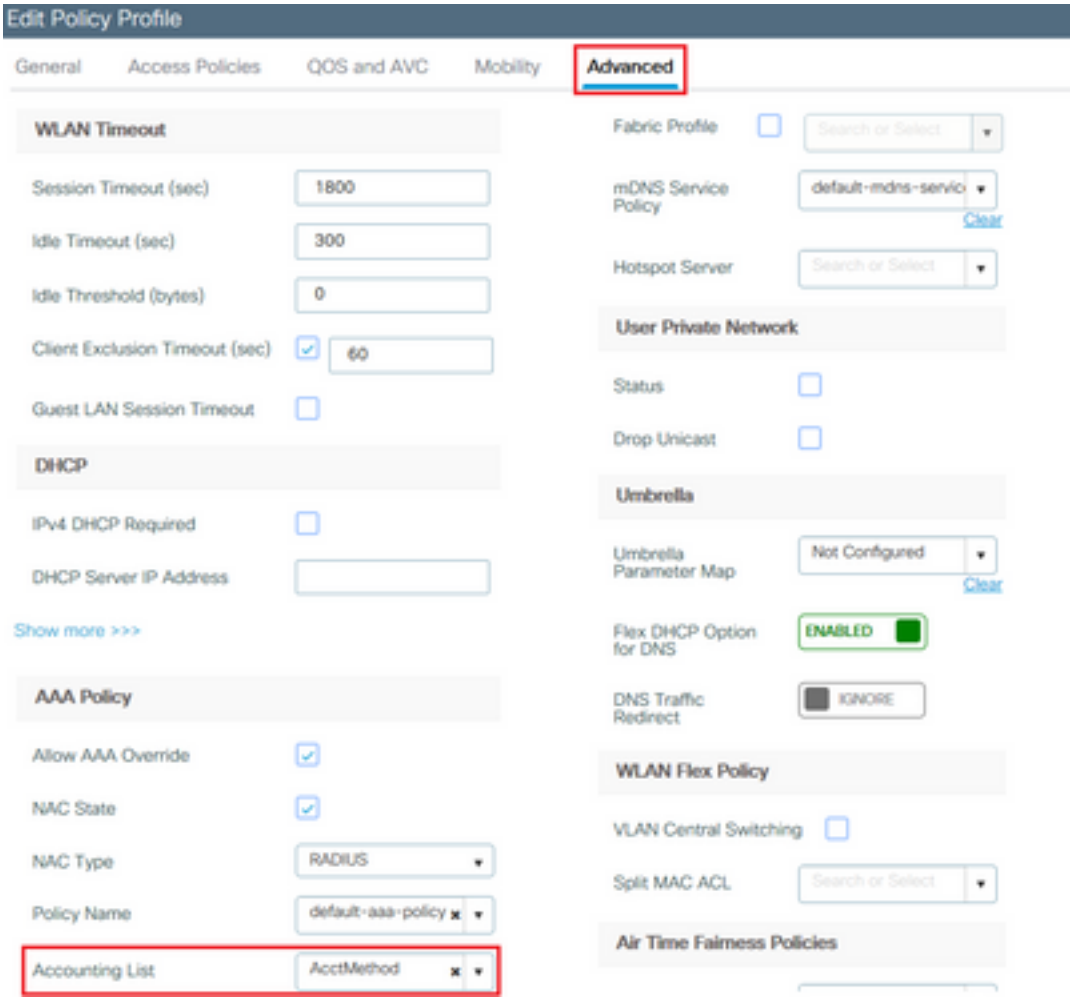
Configuración de perfiles RADIUS

Para que la creación de perfiles RADIUS funcione, además de habilitar globalmente la clasificación de dispositivos (como se menciona en la configuración de la creación de perfiles local), es necesario:

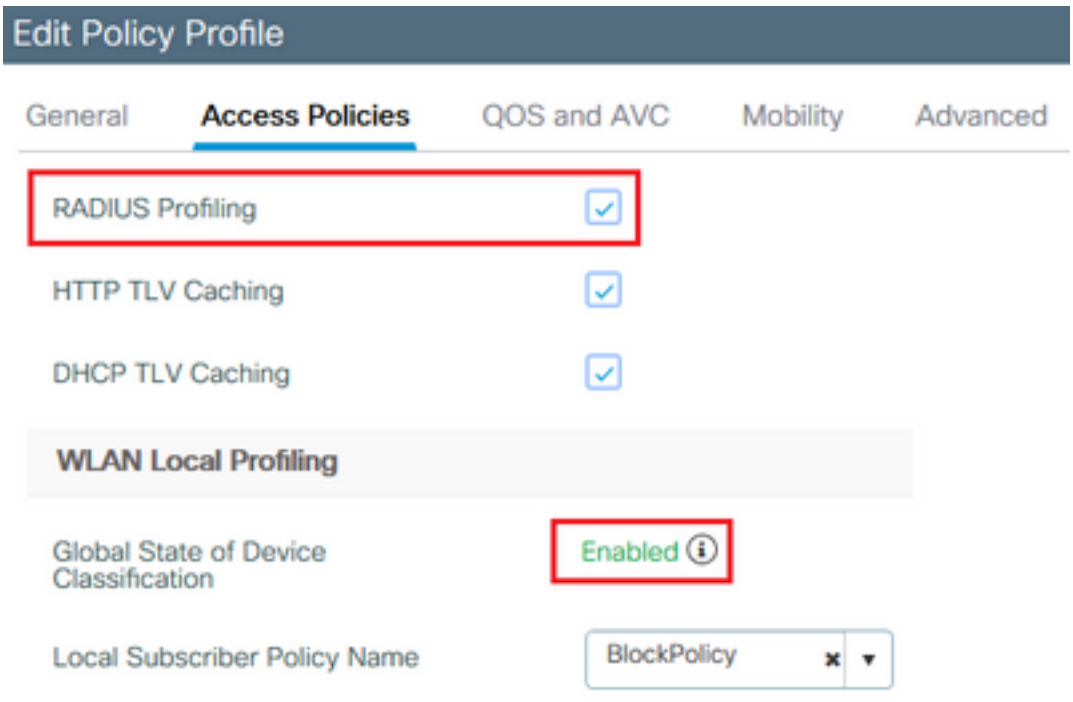
1. Configure el método de Contabilización AAA con el tipo "identidad" que apunta hacia el servidor RADIUS:



2. El método de contabilidad debe agregarse en **Configuración > Etiquetas y Perfiles > Política > [Policy_Name] > Avanzado**:



3. Por último, la casilla de verificación RADIUS Profiling debe marcarse en Configuration > Tags & Profiles > Policy . Esta casilla de verificación habilita la creación de perfiles HTTP y DHCP RADIUS (los WLC antiguos de AireOS tenían 2 casillas de verificación separadas):



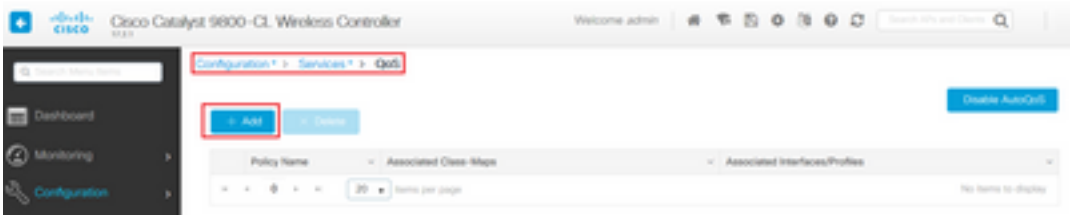
Definición de perfiles de casos prácticos

Aplicación de políticas locales basadas en la clasificación de perfiles locales

Esta configuración de ejemplo demuestra la configuración de la política local con perfil de QoS que bloquea el acceso a youtube y facebook que se aplica solamente a los dispositivos con perfil de Windows-Workstation.

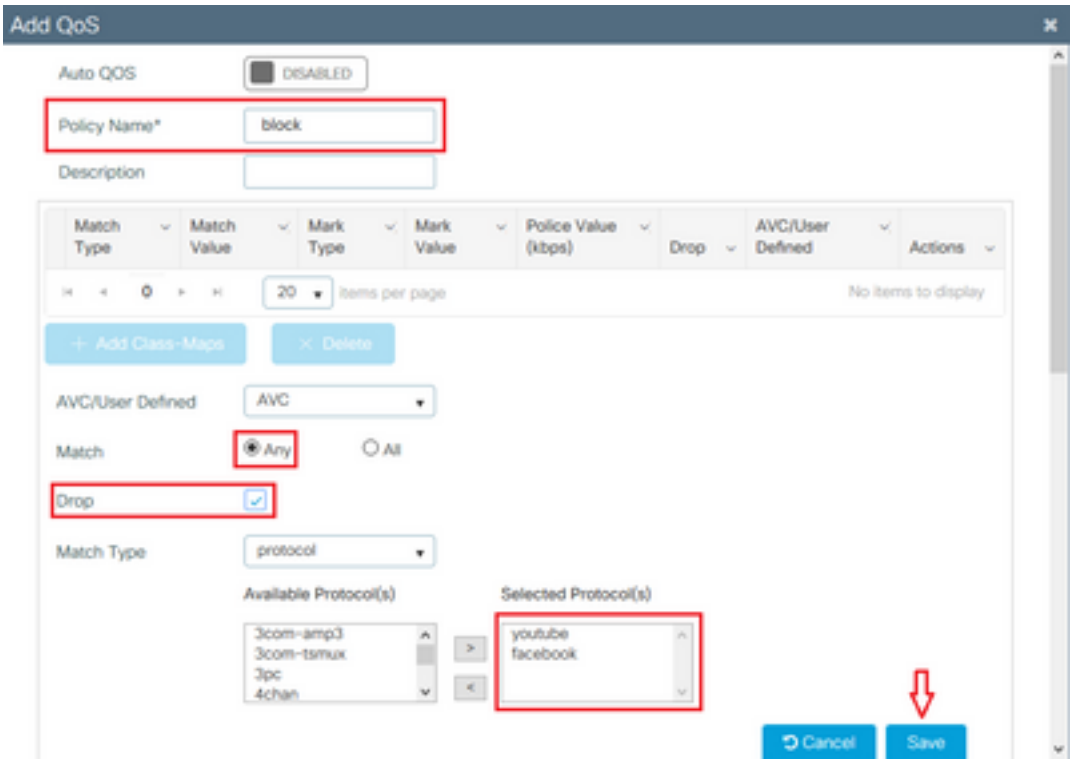
Con ligeros cambios, esta configuración se puede modificar para, por ejemplo, establecer la marcación DSCP específica sólo para teléfonos inalámbricos.

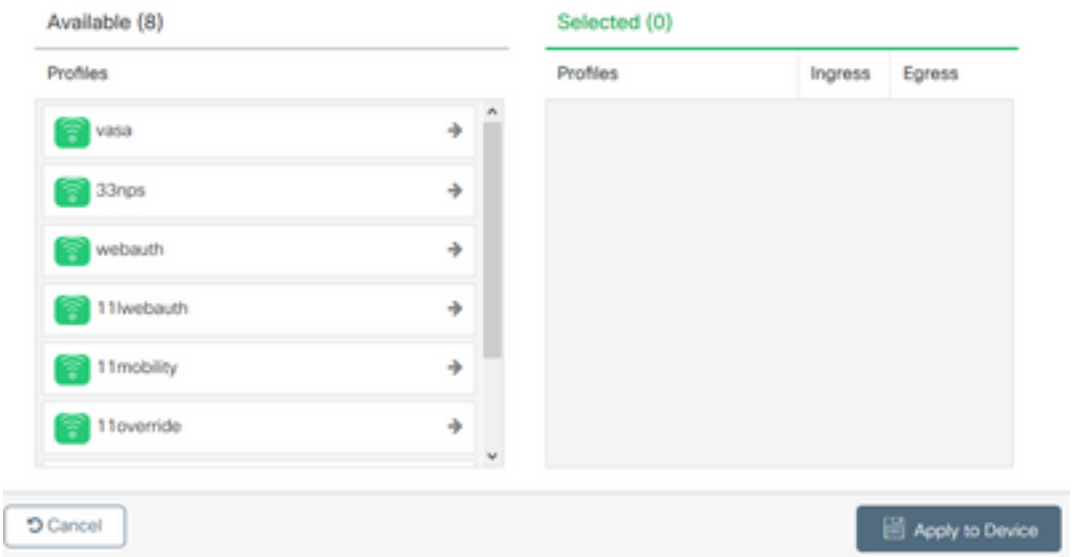
Cree un perfil de QoS navegando hasta **Configuration** > **Services** > **QoS**. Haga clic en Agregar para crear una nueva política:



Especifique el nombre de la política y agregue un nuevo mapa de clase. En los protocolos disponibles, seleccione los que deben bloquearse, DSCP marcado o ancho de banda limitado.

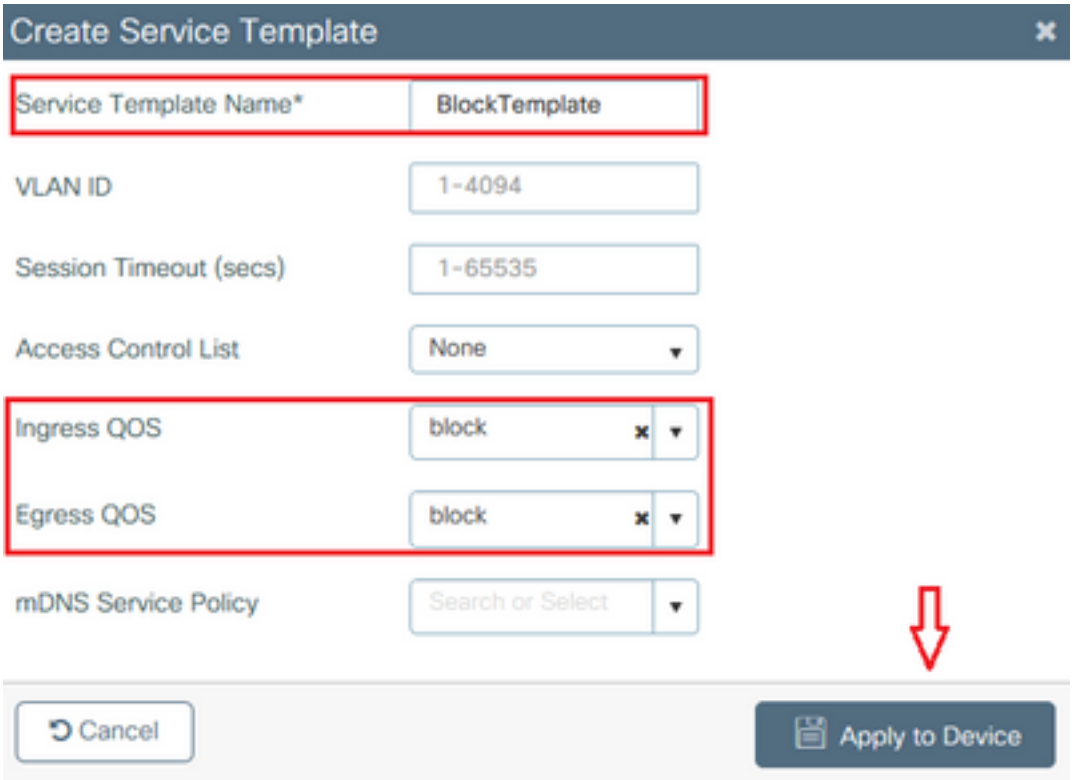
En este ejemplo, youtube y facebook están bloqueados. Asegúrese de no aplicar este perfil de QoS a ninguno de los perfiles de política en la parte inferior de la ventana QoS:





Navegue hasta **Configuration > Security > Local Policy** y cree una nueva plantilla de servicio:

Especifique el perfil de QoS de entrada y salida que se creó en el paso anterior. En este paso también se puede aplicar una lista de acceso. Si no es necesario ningún cambio de VLAN, deje el campo vlan vacío:



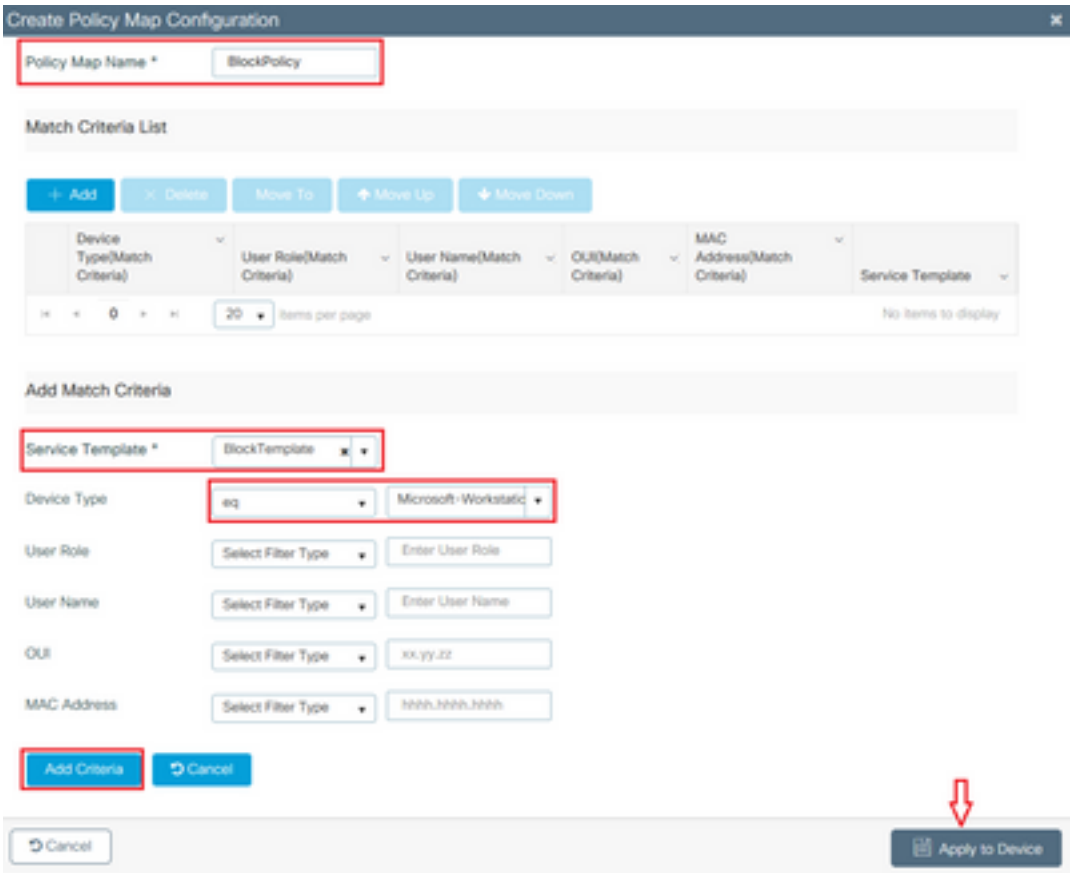
Vaya a la pestaña Policy Map y haga clic en Add:

Establezca el nombre del mapa de política y agregue nuevos criterios. Especifique la plantilla de servicio creada en el paso anterior y seleccione el tipo de dispositivo al que se aplica esta plantilla.

En este caso, se utiliza Microsoft-Workstation. Si se definen varias directivas, se utiliza la primera coincidencia.

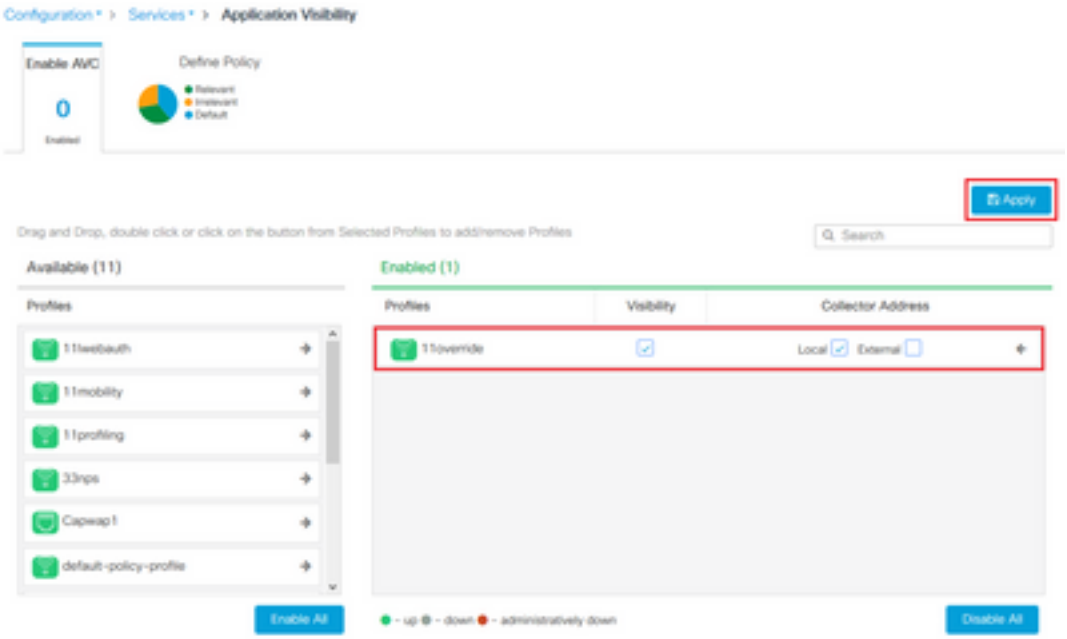
Otro caso práctico habitual sería especificar criterios de coincidencia basados en OUI. Si una implementación tiene un gran número de escáneres o impresoras del mismo modelo, normalmente tienen el mismo MAC OUI.

Esto se puede utilizar para aplicar una marcación DSCP de QoS específica o una ACL:

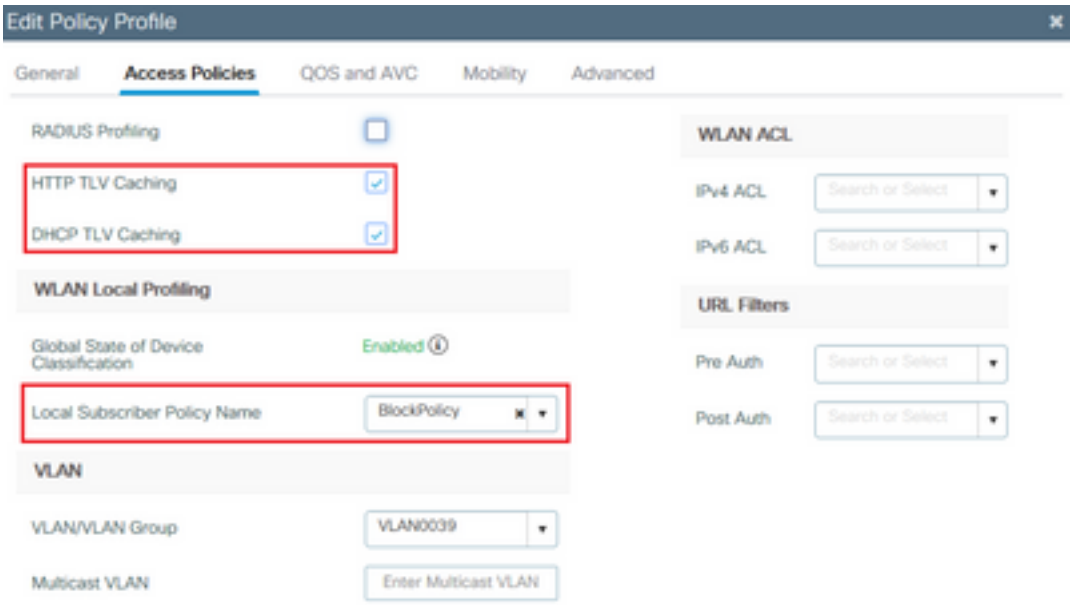


Para que el WLC pueda reconocer el tráfico de youtube y de facebook, la visibilidad de la aplicación debe ser encendida.

Vaya a **Configuration > Services > Application Visibility** eActive la visibilidad del perfil de política de su WLAN:



Verifique que bajo el perfil de la política HTTP TLV Caching, DHCP TLV Caching, Global device Classification estén habilitados y que la política de suscriptor local apunte al mapa de política local que se creó en uno de los pasos anteriores:



Una vez que el cliente se conecta, es posible comprobar si se ha aplicado la política local y comprobar si youtube y facebook están realmente bloqueados.

El resultado del comando show wireless client mac-address [MAC_ADDR] detailed contiene:

```
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
```

Definición de perfiles de RADIUS para conjuntos de políticas avanzadas en Cisco ISE

Con la creación de perfiles de RADIUS habilitada, el WLC reenvía la información de creación de perfiles al ISE. En función de esta información, es posible crear reglas avanzadas de autenticación y autorización.

Este artículo no trata sobre la configuración de ISE. Consulte la Guía de diseño de perfiles de Cisco ISE para obtener más información.

Este flujo de trabajo generalmente requiere el uso de CoA, así que asegúrese de que esté habilitado en el WLC 9800.

Definición de perfiles en implementaciones de FlexConnect

Autenticación central, conmutación local

En esta configuración, tanto la creación de perfiles local como RADIUS continúa funcionando exactamente como se describe en los capítulos anteriores. Si el AP entra en el modo autónomo (AP pierde la conexión al WLC), la definición de perfiles del dispositivo deja de funcionar y no se pueden conectar nuevos clientes.

Autenticación local, conmutación local

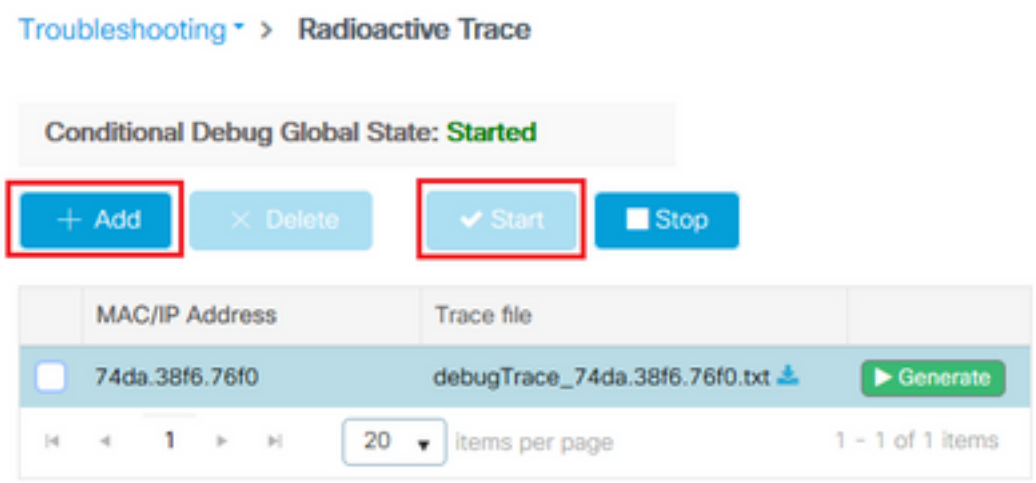
Si el AP está en el modo conectado (AP unido al WLC), el perfilado continúa funcionando (AP envía una copia de los paquetes DHCP del cliente al WLC para realizar el proceso de perfilado).

A pesar de que la generación de perfiles funciona, dado que la autenticación se realiza localmente en el AP, la información de generación de perfiles no se puede utilizar para ninguna configuración de política local o reglas de generación de perfiles RADIUS.

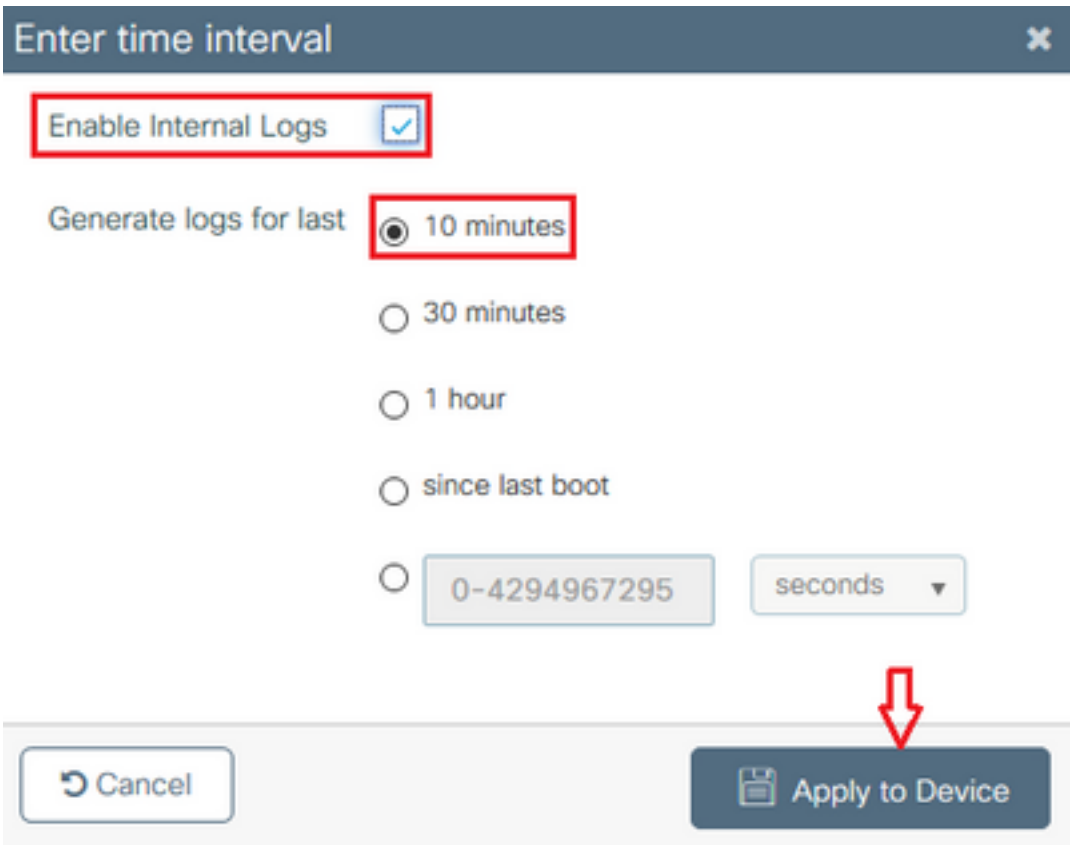
Resolución de problemas

Trazas radiactivas

La manera más fácil de resolver problemas de perfiles de cliente en el WLC es a través de rastros radiactivos. Vaya a **Troubleshooting > Radioactive Trace**, ingrese la dirección MAC del adaptador inalámbrico del cliente y haga clic en Start:



Conecte el cliente a la red y espere hasta que alcance el estado de ejecución. Detenga los seguimientos y haga clic en **Generar**. Asegúrese de que los registros internos estén habilitados (esta opción sólo existe en las versiones 17.1.1 y posteriores):



A continuación se pueden encontrar fragmentos relevantes del rastro radiactivo:

El cliente que consigue perfilado por el WLC como 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 que almacena en caché la clasificación del dispositivo:

```
(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 que encuentra la clasificación del dispositivo dentro de la memoria caché:

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

WLC que aplica la política local basada en la clasificación:

```
(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
```

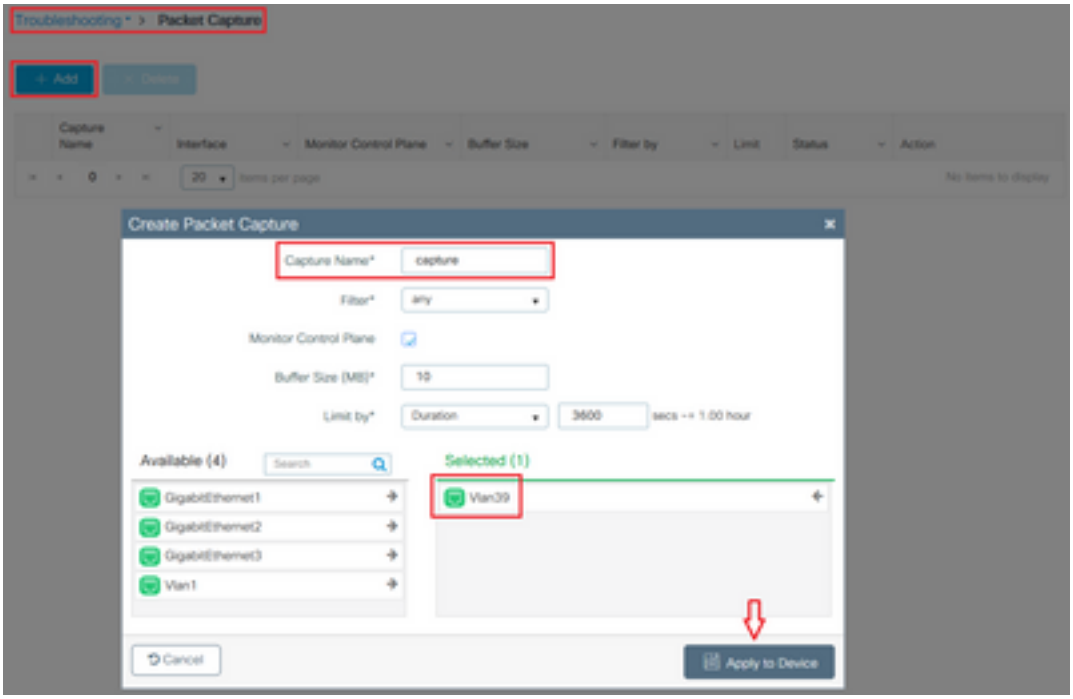
WLC que envía paquetes de contabilización que contienen DHCP y el atributo de perfilado HTTP:

```
[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
```

Capturas de paquetes

En una implementación conmutada centralmente, las capturas de paquetes se pueden realizar en el propio WLC. Navegue hasta **Troubleshooting > Captura de paquetes** y cree un nuevo punto de captura en una de las interfaces que está utilizando este cliente.

Se requiere tener SVI en la VLAN para realizar la captura en ella; de lo contrario, tome la captura en el propio puerto físico


Troubleshooting
Packet Capture
Add
Delete
Capture Name
Interface
Monitor Control Plane
Buffer Size
Filter by
Limit
Status
Action
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)
Search
GigabitEthernet1
GigabitEthernet2
GigabitEthernet3
Vlan1
Selected (1)
Vlan39
Cancel
Apply to Device

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).