

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

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Proceso de definición de perfiles](#)

[Perfiles OUI de direcciones MAC](#)

[Problemas de Direcciones MAC Administradas Localmente](#)

[Perfiles DHCP](#)

[1. Opción 12: Nombre de host](#)

[2. Opción 60: identificador de clase de proveedor](#)

[3. Opción 55 - Lista de solicitudes de parámetros](#)

[4. Opción 77 - Clase de usuario](#)

[Perfiles HTTP](#)

[Perfiles RADIUS](#)

[Perfiles DHCP RADIUS](#)

[Perfiles HTTP RADIUS](#)

[Configuración de perfiles en 9800 WLC](#)

[Configuración de perfiles locales](#)

[Configuración de perfiles RADIUS](#)

[Definición de perfiles de casos prácticos](#)

[Aplicación de políticas locales basadas en la clasificación de perfiles locales](#)

[Perfiles RADIUS para conjuntos de políticas avanzadas en Cisco ISE](#)

[Definición de perfiles en implementaciones de FlexConnect](#)

[Autenticación central, conmutación local](#)

[Autenticación local, conmutación local](#)

[Resolución de problemas](#)

[Trazas radiactivas](#)

[Capturas de paquetes](#)

[Información Relacionada](#)

Introducción

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

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- 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 Identificador único organizativo (OUI) 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:

<#root>

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:

```
<#root>
```

```
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:

No.	Time	Source	Destination	Protocol	Length	Info
376	476.758338	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1e69cc75
> Ethernet II, Src: EdimaxTe_f6:76:f0 (74:cd:a: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:cd:a: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-618289A						

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

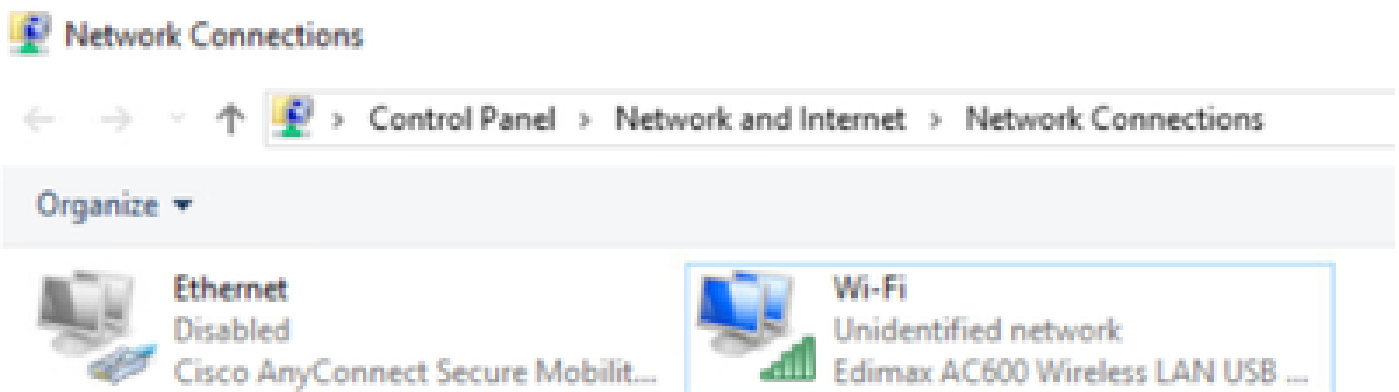
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request 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:

```
  ▾ 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]
```

Perfiles HTTP

La generación de perfiles HTTP es la forma más avanzada de generar perfiles que admite el WLC 9800 y ofrece la clasificación de dispositivos más detallada. Para que un cliente tenga perfiles HTTP, debe estar en estado de ejecución y realizar una solicitud GET HTTP. El WLC intercepta la solicitud y busca en el campo User-Agent en la cabecera 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 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 lo está, el WLC entonces realiza la interceptación necesaria para realizar el resto de la autenticación. Este HTTP GET inicial no es el único WLC que puede utilizar para perfilar el dispositivo. Cada solicitud HTTP subsiguiente es inspeccionada por el WLC y posiblemente resulte 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 connectivitycheck.gstatic.com.

Las capturas de paquetes del cliente 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:

No.	Time	Source	Destination	Protocol	Length	Info
32	11.239752	10.40.39.235	64.102.6.247	DNS	83	Standard query 0x0001 AAAA www.msftconnecttest.com
40	11.244057	64.102.6.247	10.40.39.235	DNS	249	Standard query response 0x0001 A www.msftconnecttest.com CNAME vlnco
55	11.354877	10.40.39.235	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
79	11.370009	13.107.4.52	10.40.39.235	HTTP	624	HTTP/1.1 200 OK (text/plain)

```

> Frame 55: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{76A500B3-0A27-4F03-B712-000446000000}, id 0
> Ethernet II, Src: E81aa37a_f876c9f0 [76da:38:f8:76:c9:f0], Dst: Cisco_20:41:1e:1 (24:7e:12:10:41:1e)
> Internet Protocol Version 4, Src: 10.40.39.235, Dst: 13.107.4.52
> Transmission Control Protocol, Src Port: 56815, 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 MSIE/r/n
    Host: www.msftconnecttest.com/r/n
    /r/n
    [Full request URI: http://www.msftconnecttest.com/connecttest.txt]
    [HTTP request 1/1]
    [Response in frame 79]

```

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

```
<#root>
```

```
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 métodos utilizados para clasificar el dispositivo, no hay diferencia entre Local y RADIUS Profiling.

Si RADIUS Profiling está habilitado, 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 DHCP Profiling se envía al servidor RADIUS dentro de la solicitud de contabilización como un proveedor específico de RADIUS AVPair cisco-av-pair: dhcp-option=<opción DHCP>.

Ejemplo de un paquete de solicitud de contabilización que muestra AVPairs 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):

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	849.9.520998	10.40.29.212	10.40.71.92	RADIUS	763	94189	1813	Accounting-Request id=282
2	849.9.520995	10.40.71.92	10.40.29.212	RADIUS	62	1813	64189	Accounting-Response id=282
3	850.9.520995	10.40.71.92	10.40.29.212	RADIUS	62	1813	64189	Accounting-Response id=282, Duplicate Response


```

Frame 829: 763 bytes on wire (6104 bits), 763 bytes captured (6104 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)
Datagram Protocol Version 6, Src: 10.40.29.212, Dst: 10.40.71.92
User Datagram Protocol, Src Port: 94189, Dst Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 282
Length: 763
Authenticator: 2a2d940a0e79e2718f5602a0262576c1
[The response to this request is in frame 849]
Attribute Value Pairs
- AVP: e-Vendor-SpecIFid(28) l=49 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=10 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=10 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=28 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=28 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=28 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=28 v=0 vendor=ciscoSystems(R)
  Type: 28
  Length: 28
  Vendor ID: ciscoSystems (R)
  - VSA: e-Cisco-Auth(1) l=21 v=0 val=otp-opt (0x00000000000000000000000000000000)
- AVP: e-Vendor-SpecIFid(28) l=28 v=0 vendor=ciscoSystems(R)
  Type: 28
  Length: 28
  Vendor ID: ciscoSystems (R)
  - VSA: e-Cisco-Auth(1) l=21 v=0 val=otp-opt (0x00000000000000000000000000000000)
- AVP: e-Vendor-SpecIFid(28) l=28 v=0 vendor=ciscoSystems(R)
  Type: 28
  Length: 28
  Vendor ID: ciscoSystems (R)
  - VSA: e-Cisco-Auth(1) l=21 v=0 val=otp-opt (0x00000000000000000000000000000000)

```

Perfiles HTTP RADIUS

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

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 contabilidad que reenvía este valor simple al servidor RADIUS:

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
4447	2583.868999	10.40.29.212	10.40.71.92	RADIUS	766	57987	1813	Accounting-Request id=185
4454	2583.875000	10.40.71.92	10.40.29.212	RADIUS	62	1813	57987	Accounting-Response id=185
4455	2583.875000	10.40.71.92	10.40.29.212	RADIUS	62	1813	57987	Accounting-Response id=185, Duplicate Response


```

User Datagram Protocol, Src Port: 57987, Dst Port: 1813
RADIUS Protocol
Code: Accounting-Request (4)
Packet Identifier: 185
Length: 766
Authenticator: 8080a0e0f56a1446a0488287980124d
[The response to this request is in frame 4454]
Attribute Value Pairs
- AVP: e-Vendor-SpecIFid(28) l=84 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=27 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=88 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=29 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=28 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=27 v=0 vendor=ciscoSystems(R)
- AVP: e-Vendor-SpecIFid(28) l=27 v=0 vendor=ciscoSystems(R)
  Type: 28
  Length: 28
  Vendor ID: ciscoSystems (R)
  - VSA: e-Cisco-Auth(1) l=21 v=0 val=otp-opt (0x00000000000000000000000000000000)

```

Una vez que el usuario comienza a navegar por Internet y crea algunas solicitudes HTTP GET adicionales, es posible obtener más información sobre ello. WLC envía un paquete de contabilidad adicional a ISE si detecta nuevos valores User-Agent para este cliente. En este ejemplo, es posible ver que el cliente está utilizando Windows 10 de 64 bits y Firefox 76:

Configuration > Wireless > Wireless Global

Default Mobility
Domain *

default



RF Group
Name*

default

Maximum Login
Sessions Per
User*

0

Management Via
Wireless

Device
Classification

AP LAG Mode

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.

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

BlockPolicy

Configuración de perfiles RADIUS

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

1. Configure la Lista de Métodos AAA > Contabilización con el tipo identity que apunta hacia el servidor RADIUS:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

Name	Type	Group1	Group2	Group3	Group4
AccMethod	identity	RADIUS	N/A	N/A	N/A

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

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

DNS Traffic Redirect

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

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

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

BlockPolicy

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 el perfil QoS que bloquea el acceso a YouTube y Facebook que se aplica solamente a los dispositivos con el perfil 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:

The screenshot shows the 'Add QoS' configuration interface. At the top, 'Auto QoS' is disabled. The 'Policy Name' is 'block'. The 'Drop' checkbox is checked. Under 'Selected Protocol(s)', 'youtube' and 'facebook' are listed. The 'Available (8)' section shows various profiles like 'vodafone', '33nps', 'webauth', etc. The 'Selected (0)' section is empty. A red arrow points to the 'Save' button.

Available (8)

Profiles
vodafone
33nps
webauth
11webauth
11mobility
11override

Selected (0)

Profiles	Ingress	Egress
----------	---------	--------

Cancel Save

Cancel Apply to Device

Vaya a Configuration > Security > Local Policy y cree una nueva plantilla de servicio:

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	

20 items per page 1 - 5 of 5 items

Especifique los perfiles Ingress QoS y Egress QoS que se crearon 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 ID vacío:

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



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

Service Template

Policy Map



Establezca el nombre del Policy Map 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:

Create Policy Map Configuration

Policy Map Name *

Match Criteria List

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					

Add Match Criteria

Service Template *

Device Type

User Role

User Name

OUI

MAC Address

Para que el WLC pueda reconocer el tráfico de YouTube y de Facebook, Application Visibility debe ser encendido.


Vaya a Configuration > Services > Application Visibility para habilitar la visibilidad para el perfil de política de su WLAN:

Enable AVC

0

Enabled

Define Policy



Apply

Drag and Drop, double click or click on the button from Selected Profiles to add/remove Profiles

Available (11)

Profiles	→
11fastauth	→
11mobility	→
11profiling	→
33ips	→
Classmap 1	→
default-policy-profile	→

Enable All

Enabled (1)

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

Disable All

■ - up ■ - down ■ - administratively down

Verifique que bajo el Policy Profile se habilitan las opciones HTTP TLV Caching, DHCP TLV Caching, Global device Classification y que Local Subscriber Policy Name esté señalando al policy map local que se creó en uno de los pasos anteriores:

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 BlockPolicy ▾

VLAN

VLAN/VLAN Group VLAN0039 ▾

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select ▾

IPv6 ACL Search or Select ▾

URL Filters

Pre Auth Search or Select ▾

Post Auth Search or Select ▾

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:

```
<#root>
```

```
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
```

Perfiles 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:

Troubleshooting > Radioactive Trace

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"/>

◀ 1 ▶ 20 items per page 1 - 1 of 1 items

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):

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



A continuación se pueden encontrar fragmentos relevantes del rastro radioactivo.

El cliente que consigue perfilado por el WLC como Microsoft-Workstation:

```
<#root>
```

```
2020/06/18 10:46:41.052366 {wncd_x_R0-0}{1}: [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap_9000000
```

```
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_9000000
```

```
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-Workst
```

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:

```
<#root>
```

```
(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 perfiles HTTP:

```
<#root>
```

```
[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

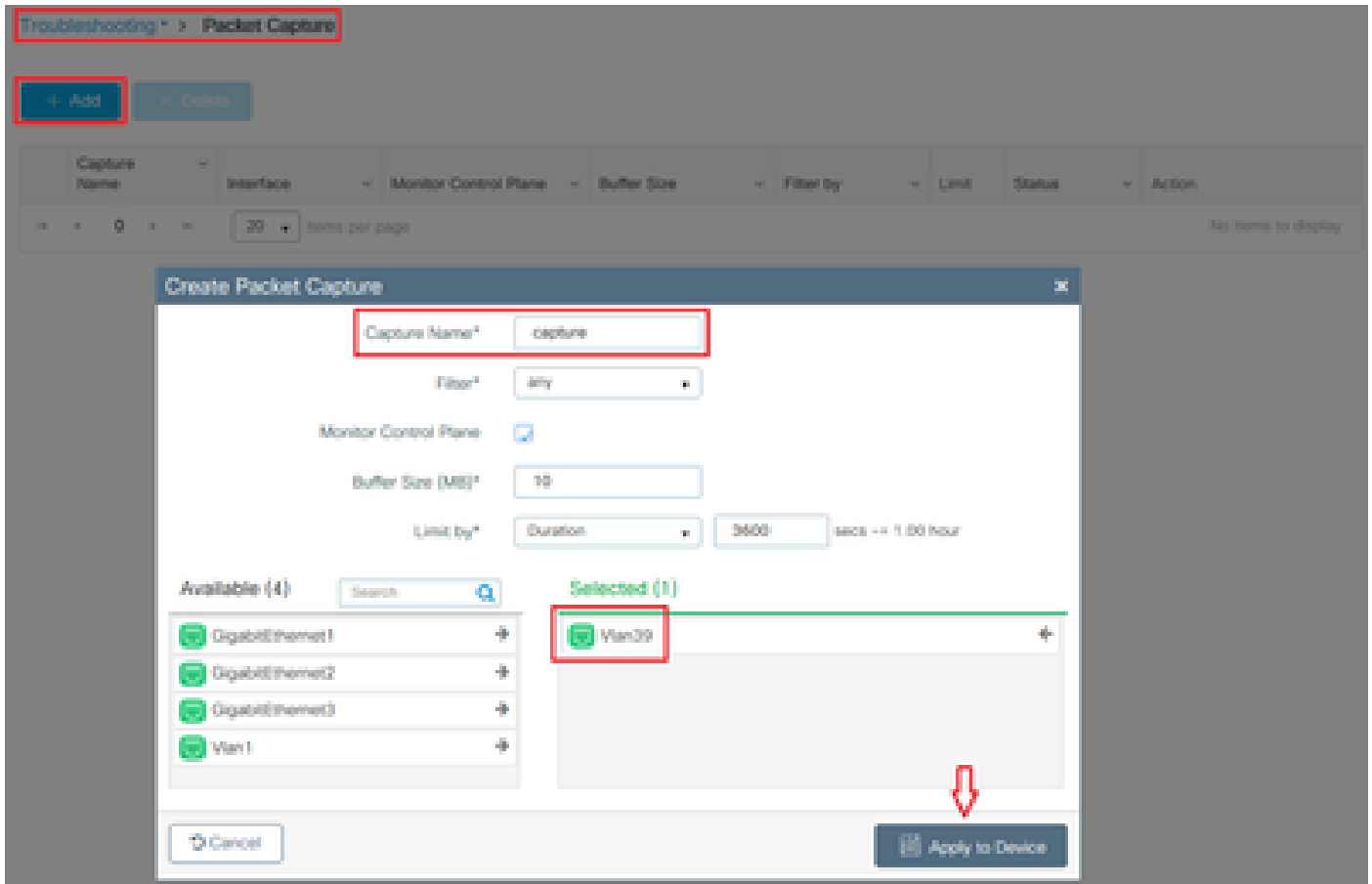
http profiling sent in a separate accounting packet

[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

Capturas de paquetes

En una implementación conmutada centralmente, las capturas de paquetes se pueden realizar en el propio WLC. Navegue hasta Troubleshooting > Packet Capture 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



Información Relacionada

- [Soporte técnico y descargas de Cisco](#)

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).