

Demonstre o perfil do cliente no controlador de LAN sem fio 9800

Contents

[Introduction](#)

[Componentes Utilizados](#)

[Processo de criação de perfil](#)

[Criação de perfil OUI de endereço MAC](#)

[Problemas de endereços MAC administrados localmente](#)

[Criação de perfil do DHCP](#)

[Criação de perfil HTTP](#)

[Criação de perfil RADIUS](#)

[Criação de perfil DHCP RADIUS](#)

[Criação de perfil HTTP RADIUS](#)

[Configurar a criação de perfil no 9800 WLC](#)

[Configuração de criação de perfil local](#)

[Configuração de criação de perfil RADIUS](#)

[Definindo o perfil dos casos de uso](#)

[Aplicando políticas locais com base na classificação de criação de perfil local](#)

[Criação de perfil Radius para conjuntos de políticas avançadas no Cisco ISE](#)

[Criação de perfis em implantações do FlexConnect](#)

[Autenticação central, comutação local](#)

[Autenticação local, comutação local](#)

[Troubleshooting](#)

[Traços radioativos](#)

[Capturas de pacotes](#)

Introduction

Este documento descreve como a classificação e a criação de perfis de dispositivos funcionam nos Cisco Catalyst 9800 Wireless LAN Controllers.

Componentes Utilizados

- 9800 CL WLC executando a imagem 17.2.1
- Access point 1815i
- Cliente sem fio Windows 10 Pro
- Cisco ISE 2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Processo de criação de perfil

Este artigo fornece uma visão detalhada de como a classificação e a criação de perfis de dispositivos funcionam nos Cisco Catalyst 9800 Wireless LAN Controllers, descreve casos de uso potenciais, exemplos de configuração e etapas necessárias para solucionar problemas.

O perfil do dispositivo é um recurso que oferece uma maneira de descobrir informações adicionais sobre um cliente sem fio que ingressou na infraestrutura sem fio.

Depois que o perfil do dispositivo é executado, ele pode ser usado para aplicar diferentes políticas locais ou para corresponder a regras específicas do servidor RADIUS.

As WLCs Cisco 9800 são capazes de executar três (3) tipos de criação de perfis de dispositivos:

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

Criação de perfil OUI de endereço MAC

O endereço MAC é um identificador exclusivo de cada interface de rede sem fio (e com fio). É um número de 48 bits normalmente escrito em formato hexadecimal MM:MM:MM:SS:SS.

Os primeiros 24 bits (ou 3 octetos) são conhecidos como OUI (Organizationally Unique Identifier) e identificam exclusivamente um fornecedor ou fabricante.

Eles são comprados e atribuídos pelo IEEE. Um fornecedor ou fabricante pode comprar vários OUIs.

Exemplo:

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

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

Quando um cliente sem fio se associa ao access point, a WLC executa a pesquisa do OUI para determinar o fabricante.

Em implantações de switching local Flexconnect, o AP ainda retransmite informações relevantes do cliente para a WLC (como pacotes DHCP e endereço MAC do cliente).

A definição de perfis baseada apenas no OUI é extremamente limitada e é possível classificar o dispositivo como uma marca específica, mas não é capaz de diferenciar entre um laptop e um smartphone.

Problemas de endereços MAC administrados localmente

Devido a preocupações com privacidade, muitos fabricantes começaram a implementar recursos de randomização mac em seus dispositivos.

Os endereços MAC administrados localmente são gerados aleatoriamente e têm um segundo bit menos significativo do primeiro octeto do endereço definido como 1.

Esse bit atua como um sinalizador que anuncia que o endereço mac é na verdade um endereço

gerado aleatoriamente.

Há quatro formatos possíveis de endereços MAC administrados localmente (x pode ser qualquer 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
```

Por padrão, os dispositivos Android 10 usam um endereço MAC administrado localmente e gerado aleatoriamente toda vez que se conectam a uma nova rede SSID.

Esse recurso anula completamente a classificação de dispositivo baseada em OUI, pois o controlador reconhece que o endereço foi aleatório e não executa nenhuma pesquisa.

Criação de perfil do DHCP

O perfil do DHCP é executado pela WLC através da investigação dos pacotes DHCP que o cliente sem fio está enviando.

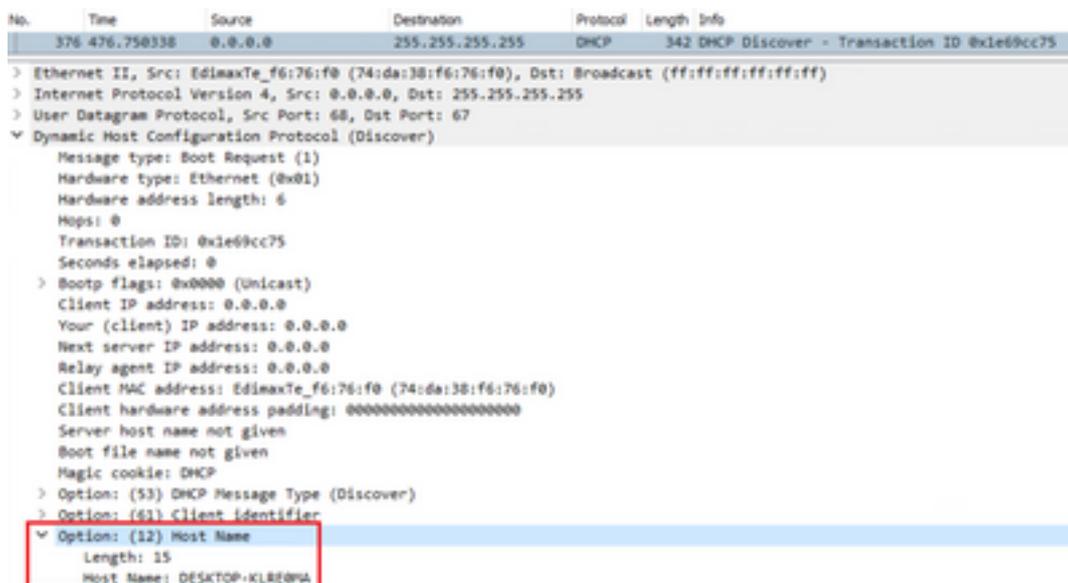
Se a criação de perfil do DHCP tiver sido usada para classificar o dispositivo, a saída do comando **show wireless client mac-address [MAC_ADDR] detailed** conterá:

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

A WLC inspeciona vários campos da Opção DHCP nos pacotes enviados por clientes sem fio:

1. Opção 12 - Nome do host

Esta opção representa o nome de host do cliente e pode ser encontrada nos pacotes DHCP Discover e DHCP Request:



```
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. Opção 60 - Identificador da Classe de Fornecedor

Essa opção também é encontrada nos pacotes DHCP Discover e Request.

Com essa opção, os clientes podem se identificar para o servidor DHCP e os servidores podem ser configurados para responder apenas aos clientes com identificador de classe de fornecedor específico.

Essa opção é mais comumente usada para identificar os pontos de acesso na rede e responder a eles apenas com a opção 43.

Exemplos de identificadores da classe de fornecedor

- "MSFT 5.0" para todos os clientes Windows 2000 (e superiores)
- "MSFT 98" para todos os clientes Windows 98 e Me
- "MSFT" para todos os clientes Windows 98, Me e 2000

Os dispositivos Apple MacBook não enviam a opção 60 por padrão.

Exemplo de captura de pacotes do cliente Windows 10:

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

3. Opção 55 - Lista de Solicitações de Parâmetros

A opção Lista de solicitações de parâmetro DHCP contém parâmetros de configuração (códigos de opção) que o cliente DHCP está solicitando do servidor DHCP. É uma string escrita em notação separada por vírgulas (por exemplo, 1,15,43).

Não é uma solução perfeita, pois os dados que produz dependem do fornecedor e podem ser duplicados por vários tipos de dispositivos.

Por exemplo, os dispositivos Windows 10 sempre solicitam, por padrão, uma determinada lista de parâmetros. Os iPhones e iPads da Apple usam diferentes conjuntos de parâmetros nos quais é possível classificá-los.

Exemplo de captura do cliente Windows 10:

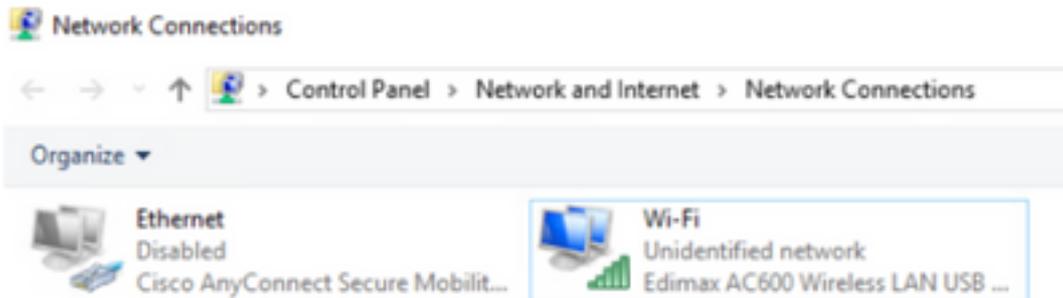
```
Option: (55) Parameter Request List
Length: 14
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter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

A classe de usuário é uma opção que geralmente não é usada por padrão e exige que o cliente seja configurado manualmente. Por exemplo, esta opção pode ser configurada em uma máquina Windows usando o comando:

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

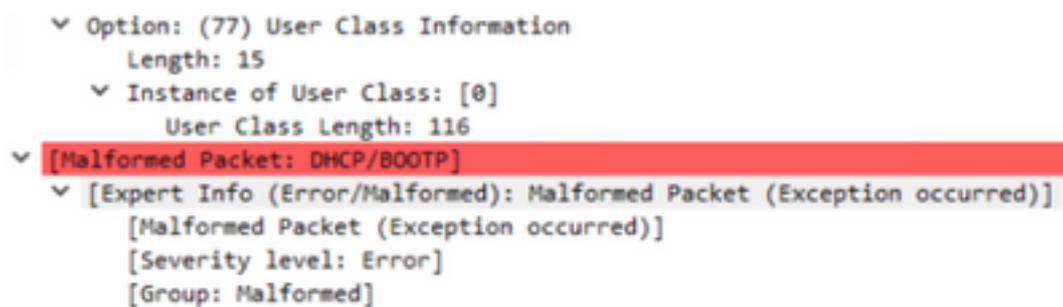
O nome do adaptador pode ser encontrado na Central de Rede e Compartilhamento no painel de controle:



Configure a opção 66 do DHCP para o cliente Windows 10 no CMD (requer direitos 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.
```

Devido à implementação da opção 66 pelo Windows, o Wireshark não é capaz de decodificar esta opção e parte do pacote que vem após a opção 66 aparece como malformado:



Criação de perfil HTTP

A criação de perfis HTTP é a maneira mais avançada de criar perfis para o 9800 WLC e oferece a classificação de dispositivo mais detalhada.

Para que um cliente tenha o perfil HTTP, ele precisa estar em um estado "Executar" e executar uma solicitação HTTP GET.

A WLC intercepta a solicitação e examina o campo "User-Agent" no cabeçalho HTTP do pacote.

Esse campo contém informações adicionais sobre o cliente sem fio que podem ser usadas para classificá-lo.

Por padrão, quase todos os fabricantes implementaram um recurso no qual um cliente sem fio tenta executar a verificação de conectividade da Internet.

Essa verificação também é usada para detecção automática do portal de convidado. Se um dispositivo recebe uma resposta HTTP com código de status 200 (OK), isso significa que a WLAN não é protegida com webauth.

Se estiver, a WLC executará a interceptação necessária para executar o restante da autenticação. Esse HTTP GET inicial não é o único que a WLC pode usar para criar o perfil do dispositivo.

Cada solicitação HTTP subsequente é inspecionada pela WLC e possivelmente resulta com uma classificação ainda mais detalhada.

Os dispositivos Windows 10 usam o domínio **msftconnecttest.com** para executar esse teste. Os dispositivos Apple usam **captive.apple.com**, enquanto os dispositivos Android geralmente usam **connectivitycheck.gstatic.com**.

As capturas de pacotes do cliente Windows 10 que executa essa verificação podem ser encontradas abaixo. O campo User Agent é preenchido com **Microsoft NCSI**, o que resulta no perfil do cliente na WLC como **Microsoft-Workstation**:

```
No.    Time          Source            Destination       Protocol  Length  Info
---    -
32    11.230352     10.48.39.235     64.182.6.247     DNS      83      Standard query 0x6d6d AAAA www.msftconnecttest.com
48    11.344857     64.182.6.247     10.48.39.235     DNS      249     Standard query response 0x6d6d A www.msftconnecttest.com CNAME vlcnc
55    11.354877     10.48.39.235     13.187.4.52      HTTP     365     GET /connecttest.txt HTTP/1.1
70    11.370009     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_{95A00002-0B27-4F05-8912-96A84E0839A8}, id 0
> Ethernet II, Src: EdimaxTe_f6:76:f9 (74:da:38:f6:76:f9), Dst: Cisco_19:41: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 1/1]
  [Response in frame 70]
```

Exemplo de saída do **show wireless client mac-address [MAC_ADDR]** detalhado para um cliente com perfil via 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
```

Criação de perfil RADIUS

Quando se trata de métodos usados para classificar o dispositivo, não há diferença entre a criação de perfil local e RADIUS.

Se a criação de perfil Radius estiver habilitada, a WLC encaminhará as informações que aprendeu sobre o dispositivo por meio de um conjunto específico de atributos RADIUS específicos do fornecedor para o servidor RADIUS.

Criação de perfil DHCP RADIUS

As informações obtidas através da criação de perfis de DHCP são enviadas ao servidor RADIUS dentro da solicitação de contabilidade como um RADIUS AVPair específico do fornecedor **cisco-**


```
4744 1995,180880 18.48.39.112 18.48.71.92 AADIUS 765 57397 1813 Accounting-Request Id=186
4749 1995,111994 18.48.71.92 18.48.39.112 AADIUS 62 1813 57397 Accounting-Response Id=186
4758 1995,111994 18.48.71.92 18.48.39.112 AADIUS 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: 4885c8d8b8eae7862d5837f9844f2f
[The response to this request is in frame 4763]
Attribute Value Pairs
  > AVP: t=Vendor-Specific(26) 1444 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1437 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1448 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1429 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1438 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1426 vnd=ciscoSystems(P)
  > AVP: t=Vendor-Specific(26) 1499 vnd=ciscoSystems(P)
    Type: 26
    Length: 99
    Vendor ID: ciscoSystems (9)
    > VSA: t=Cisco-APPair(1) 1=93 val=http-tls=1000/00100000001111/5.8 [Windows NT 10.0; x64; rv:76.0] Gecko/20100101 Firefox/76.0
```

Configurar a criação de perfil no 9800 WLC

Configuração de criação de perfil local

Para que a criação de perfil local funcione, basta habilitar a Classificação do dispositivo em Configuração > Sem fio > Global sem fio. Esta opção habilita o perfil MAC OUI, HTTP e DHCP ao mesmo tempo:

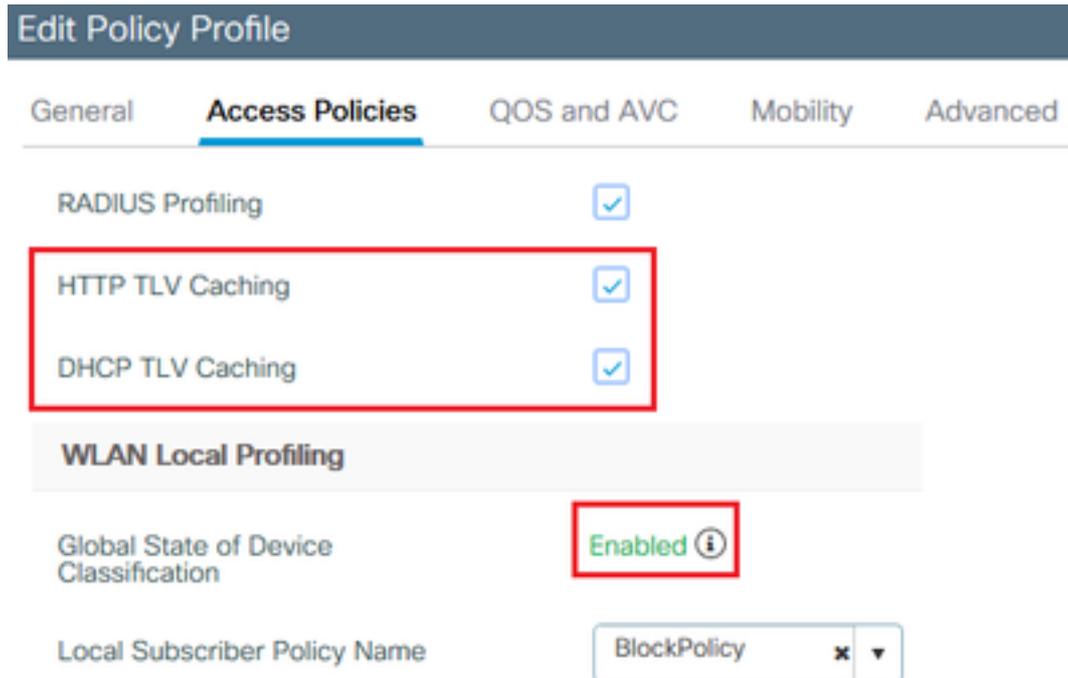
Configuration > Wireless > Wireless Global

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

Além disso, na configuração Política, você pode habilitar o Cache TLV HTTP e o Cache TLV DHCP. A WLC executa a criação de perfis mesmo sem eles.

Com essas opções ativadas, a WLC armazena em cache as informações aprendidas

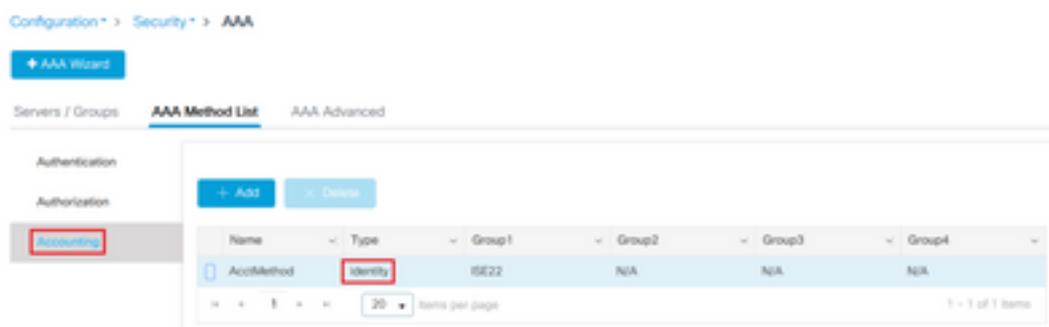
anteriormente sobre esse cliente e evita a necessidade de inspecionar pacotes adicionais gerados por esse dispositivo.



Configuração de criação de perfil RADIUS

Para que a criação de perfil RADIUS funcione, além de habilitar globalmente a classificação do dispositivo (como mencionado na configuração de Criação de Perfil Local), é necessário:

1. Configure o método de contabilização AAA com o tipo "identidade" apontando em direção ao servidor RADIUS:



2. O método de contabilização precisa ser adicionado em **Configuration > Tags & Profiles > Policy > [Policy_Name] > Advanced**:

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. Finalmente, RADIUS Profiling caixa de verificação precisa ser marcada em Configuration > Tags & Profiles > Policy Esta caixa de verificação habilita tanto HTTP e DHCP RADIUS profiling (AireOS WLCs antigos tinha 2 caixas de verificação 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

Definindo o perfil dos casos de uso

Aplicando políticas locais com base na classificação de criação de perfil local

Esta configuração de exemplo demonstra a configuração da Diretiva Local com perfil de QoS bloqueando o acesso ao Youtube e facebook que é aplicado somente a dispositivos com perfil Windows-Workstation.

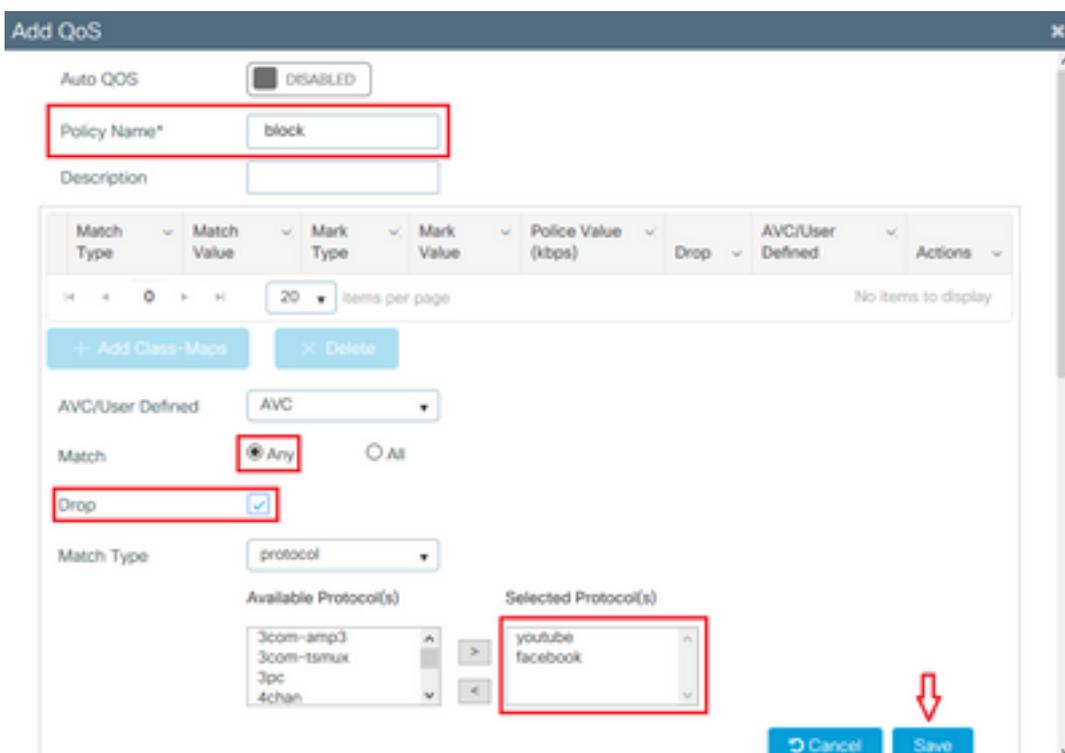
Com pequenas alterações, essa configuração pode ser modificada para, por exemplo, definir a marcação de DSCP específica apenas para telefones sem fio.

Crie um perfil de QoS navegando até **Configuration > Services > QoS**. Clique em Adicionar para criar uma nova política:



Especifique o nome da política e adicione um novo mapa de classe. Nos protocolos disponíveis, selecione aqueles que precisam ser bloqueados, marcados com DSCP ou com largura de banda limitada.

Neste exemplo, o Youtube e o facebook estão bloqueados. Certifique-se de não aplicar este perfil de QoS a nenhum dos perfis de política na parte inferior da janela QoS:



Available (8) Selected (0)

Profiles

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

Cancel Apply to Device

Navegue até **Configuration > Security > Local Policy** e crie um novo Service Template:

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

Especifique o perfil de QoS de entrada e saída criado na etapa anterior. Uma lista de acesso também pode ser aplicada nesta etapa. Se nenhuma alteração de VLAN for necessária, deixe o campo vlan vazio:

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



Navegue até a guia Mapa de políticas e clique em adicionar:

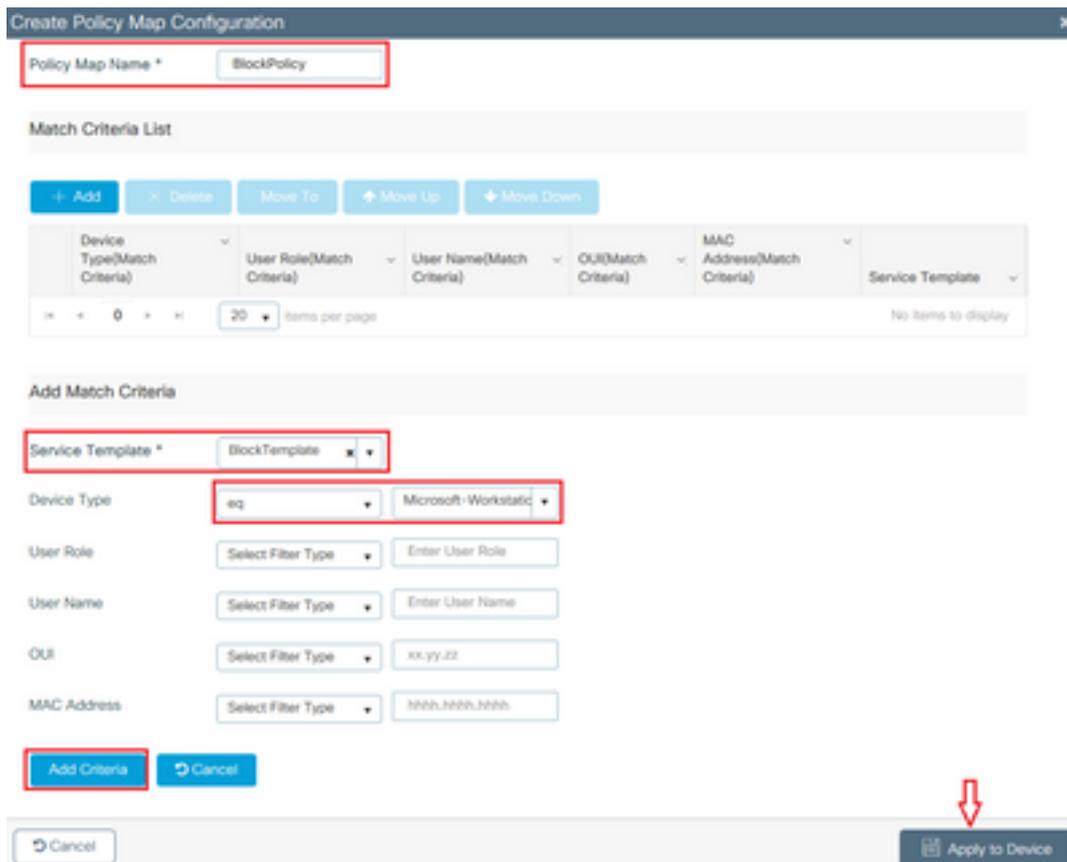


Defina o nome do Mapa de Políticas e adicione novos critérios. Especifique o Modelo de serviço que foi criado na etapa anterior e selecione o Tipo de dispositivo ao qual esse modelo está aplicado.

Nesse caso, é usado o Microsoft Workstation. Se várias políticas forem definidas, a primeira correspondência será usada.

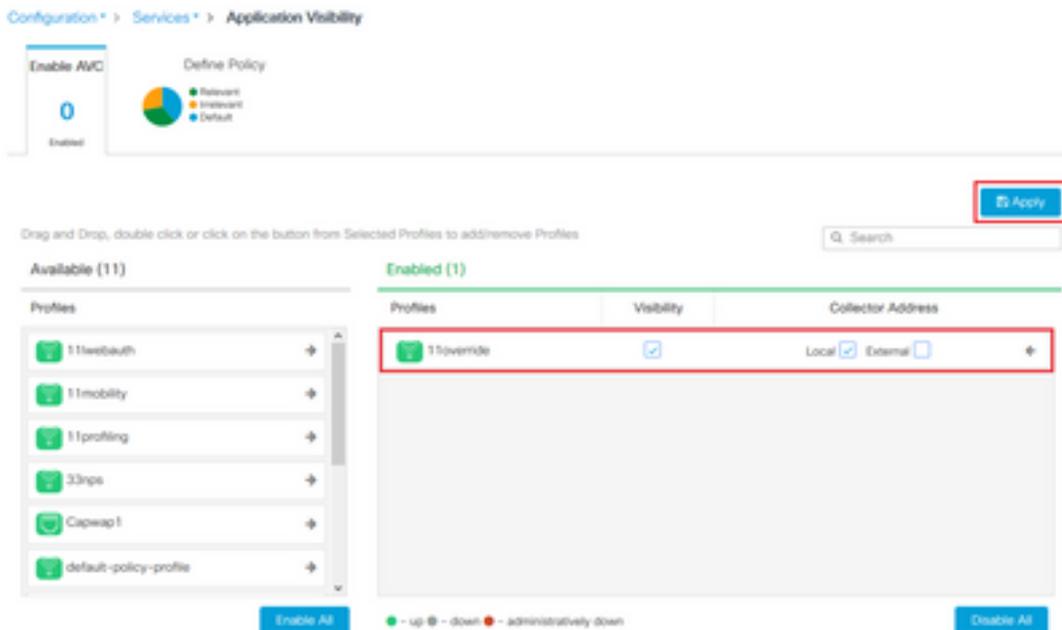
Um outro caso de uso comum seria especificar critérios de correspondência baseados em OUI. Se uma implantação tiver um grande número de scanners ou impressoras do mesmo modelo, eles geralmente terão o mesmo MAC OUI.

Isso pode ser usado para aplicar a marcação QoS DSCP específica ou uma ACL:

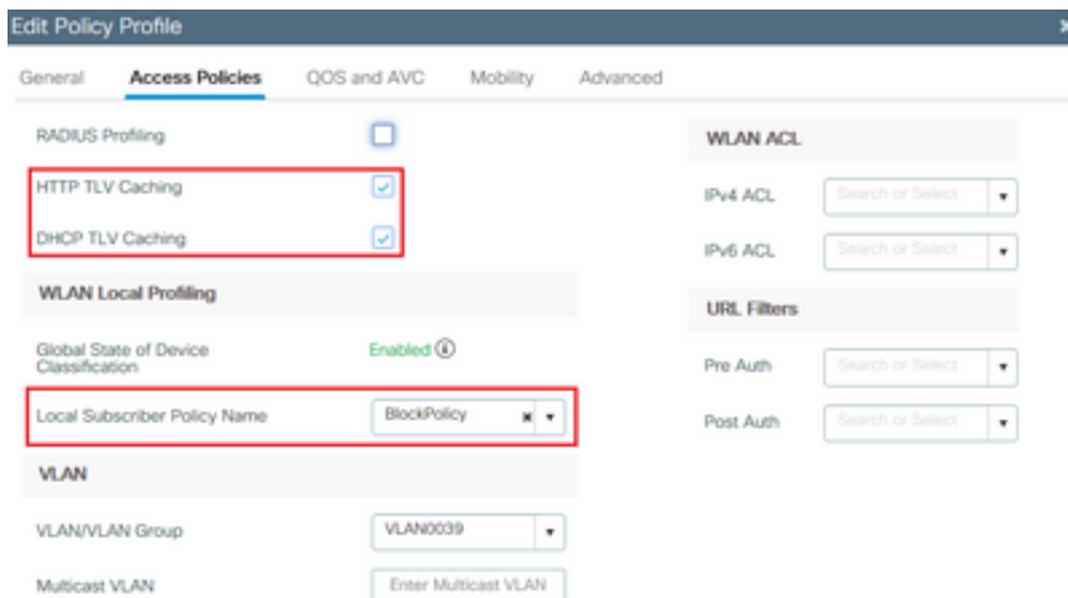


Para que a WLC possa reconhecer o tráfego do YouTube e do Facebook, a visibilidade do aplicativo precisa estar ativada.

Navegue até **Configuration > Services > Application Visibility** e Habilite a visibilidade para o perfil de política da sua WLAN:



Verifique se, em Perfil da política, o Cache TLV HTTP, o Cache TLV DHCP e a Classificação de dispositivo global estão habilitados e se a Política de assinante local está apontando para o mapa de Política local que foi criado em uma das etapas anteriores:



Depois que o cliente se conecta, é possível verificar se a política local foi aplicada e testar se o youtube e o facebook estão realmente bloqueados.

A saída do comando show wireless client mac-address [MAC_ADDR] detailed contém:

```

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
```

Criação de perfil Radius para conjuntos de políticas avançadas no Cisco ISE

Com a criação de perfil RADIUS ativada, a WLC encaminha as informações de criação de perfil para o ISE. Com base nessas informações, é possível criar regras avançadas de autenticação e autorização.

Este artigo não aborda a configuração do ISE. Consulte o [Guia de design de criação de perfil do Cisco ISE](#) para obter mais informações.

Esse fluxo de trabalho geralmente requer o uso de CoA, portanto, certifique-se de que ele esteja habilitado na WLC 9800.

Criação de perfis em implantações do FlexConnect

Autenticação central, comutação local

Nesta configuração, tanto o perfil local quanto o RADIUS continuam a funcionar exatamente como descrito nos capítulos anteriores. Se o AP entrar no modo autônomo (o AP perde a conexão com a WLC), o perfil do dispositivo para de funcionar e nenhum cliente novo pode se conectar.

Autenticação local, comutação local

Se o AP estiver no modo conectado (AP unido à WLC), a criação de perfil continuará a funcionar (o AP envia uma cópia dos pacotes DHCP do cliente para a WLC para executar o processo de criação de perfil).

Apesar da criação de perfil funcionar, já que a autenticação é realizada localmente no AP, as informações de criação de perfil não podem ser utilizadas para qualquer configuração de política local ou regras de criação de perfil RADIUS.

Troubleshooting

Traços radioativos

A maneira mais fácil de solucionar problemas de criação de perfis de clientes na WLC é por meio de rastreamentos radioativos. Navegue para **Troubleshooting > Radioative Trace**, insira o endereço MAC do adaptador sem fio do cliente e clique em Start:

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

Conecte o cliente à rede e aguarde até que ele atinja o estado de execução. Pare os rastreamentos e clique em **Gerar**. Certifique-se de que os registros internos estejam ativados (esta opção só existe nas versões 17.1.1 e superiores):

Enter time interval ×

Enable Internal Logs

Generate logs for last 10 minutes

30 minutes

1 hour

since last boot

Os fragmentos relevantes do traço radioativo podem ser encontrados abaixo:

O cliente sendo perfilado pelo 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
    
```

Classificação do dispositivo no cache da WLC:

```
(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
```

A WLC está descobrindo a classificação do dispositivo dentro do cache:

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

WLC aplicando a política local com base na classificação:

```
(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
```

A WLC está enviando pacotes de contabilização que contêm o atributo de perfil DHCP e 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 pacotes

Em uma implantação comutada centralmente, as capturas de pacotes podem ser executadas na própria WLC. Navegue para **Troubleshooting > Captura de Pacotes** e crie um novo ponto de captura em uma das interfaces que estão em uso por este cliente.

É necessário ter o SVI na vlan para executar a captura nela, caso contrário, faça a captura na própria porta física

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.