# 9800ワイヤレスLANコントローラでのクライア ントプロファイリングのデモ

# 内容

### <u>概要</u>

使用するコンポーネント プロファイルプロセス MACアドレスOUIプロファイリング ローカルで管理されるMACアドレスの問題 DHCPプロファイリング HTTPプロファイリング RADIUSプロファイリング DHCP RADIUSプロファイリング HTTP RADIUSプロファイリング 9800 WLCでのプロファイリングの設定 ローカルプロファイリング設定 RADIUSプロファイリングの設定 プロファイリングの使用例 ローカルプロファイリング分類に基づくローカルポリシーの適用 Cisco ISEの高度なポリシーセットのRADIUSプロファイリング FlexConnectの導入におけるプロファイリング 中央認証、ローカル スイッチング ローカル認証、ローカル スイッチング トラブルシューティング 放射能痕跡 パケット キャプチャ

## 概要

このドキュメントでは、Cisco Catalyst 9800ワイヤレスLANコントローラでのデバイス分類とプ ロファイリングの動作について説明します。

## 使用するコンポーネント

- •17.2.1イメージを実行する9800 CL WLC
- •1815iアクセスポイント
- Windows 10 Proワイヤレスクライアント
- Cisco ISE 2.7

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

# プロファイルプロセス

この記事では、Cisco Catalyst 9800ワイヤレスLANコントローラでデバイスの分類とプロファイ リングがどのように機能するかについて詳しく説明し、潜在的な使用例、設定例、およびトラブ ルシューティングに必要な手順について説明します。

デバイスプロファイリングは、ワイヤレスインフラストラクチャに参加したワイヤレスクライア ントに関する追加情報を見つける方法を提供する機能です。

デバイスのプロファイリングが実行されると、そのプロファイルを使用してさまざまなローカル ポリシーを適用したり、特定のRADIUSサーバルールに一致させることができます。

Cisco 9800 WLCは、次の3種類のデバイスプロファイリングを実行できます。

1. MACアドレスOUI

2. DHCP

3. HTTP

### MACアドレスOUIプロファイリング

MACアドレスは、各ワイヤレス(および有線)ネットワークインターフェイスの一意の識別子で す。通常は48ビットの数値で、16進数形式(MM:MM:SS:SS:SS)で表記されます。

最初の24ビット(または3オクテット)はOUI(Organizational Unique Identifier)と呼ばれ、ベンダーまたは製造元を一意に識別します。

これらはIEEEから購入され、IEEEによって割り当てられます。1つのベンダーまたは製造業者が 複数のOUIを購入できます。

例:

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

ワイヤレスクライアントがアクセスポイントに関連付けられると、WLCはOUIルックアップを実行して製造元を特定します。

Flexconnectローカルスイッチングの導入では、APは引き続き関連クライアント情報(DHCPパケットやクライアントMACアドレスなど)をWLCにリレーします。

OUIのみに基づくプロファイリングは非常に限られており、デバイスを特定のブランドとして分類することは可能ですが、ラップトップとスマートフォンを区別することはできません。

#### ローカルで管理されるMACアドレスの問題

プライバシーの問題が原因で、多くのメーカーがMACランダム化機能をデバイスに実装し始めました。

ローカルで管理されるMACアドレスはランダムに生成され、アドレスの最初のオクテットの2番目の最下位ビットが1に設定されます。

このビットは、MACアドレスが実際にはランダムに生成されたものであることを通知するフラグ として機能します。 ローカルで管理されるMACアドレスには、次の4つの形式があります(xは任意の16進数値です )。

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

Android 10デバイスは、デフォルトで、新しいSSIDネットワークに接続するたびに、ランダムに 生成されたローカル管理MACアドレスを使用します。

この機能は、アドレスがランダム化されたことをコントローラが認識し、ルックアップを実行しないため、OUIベースのデバイス分類を完全に無効にします。

### DHCPプロファイリング

DHCPプロファイリングは、ワイヤレスクライアントが送信しているDHCPパケットを調査する ことによってWLCによって実行されます。

DHCPプロファイリングを使用してデバイスを分類した場合、show wireless client mac-address [MAC\_ADDR] detailedコマンドの出力には次が含まれます。

Device Type : Microsoft-Workstation Device Name : MSFT 5.0 Protocol Map : 0x00009 (OUI, DHCP) Protocol : DHCP WLCは、ワイヤレスクライアントから送信されるパケットの中のいくつかのDHCPオプションフ ィールドを検査します。

#### 1.オプション12:ホスト名

このオプションはクライアントのホスト名を表し、DHCP DiscoverおよびDHCP Requestパケットで確認できます。



### 2.オプション60:ベンダークラスID

このオプションは、DHCP DiscoverおよびRequestパケットにも含まれています。

このオプションを使用すると、クライアントはDHCPサーバに対して自身を識別し、特定のベン ダークラスIDを持つクライアントにのみ応答するようにサーバを設定できます。

このオプションは、ネットワーク内のアクセスポイントを特定し、それに対してオプション43でのみ応答するために最も一般的に使用されます。

ベンダークラスIDの例

• "MSFT 5.0" すべてのWindows 2000クライアント(以降)

• "MSFT 98" すべてのWindows 98およびMeクライアント用

•「**MSFT**」 すべてのWindows 98、Me、および2000クライアント用

Apple MacBookデバイスは、デフォルトではオプション60を送信しません。

Windows 10クライアントからのパケットキャプチャ例:

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

#### 3.オプション55:パラメータ要求リスト

[DHCPパラメータ要求リスト(DHCP Parameter Request List)]オプションには、DHCPクライアン トがDHCPサーバに要求する設定パラメータ(オプションコード)が含まれています。カンマ区 切り形式で記述された文字列です(例:1,15,43)。

生成されるデータはベンダーに依存し、複数のデバイスタイプで複製できるため、完全なソリュ ーションではありません。

たとえば、Windows 10デバイスは常にデフォルトで特定のパラメータリストを要求します。 AppleのiPhoneとiPadは、異なるパラメータセットを使用し、それらを分類することができます 。

Windows 10クライアントからのキャプチャ例:

```
Option: (55) Parameter Request List
   Length: 14
   Parameter Request List Item: (1) Subnet Mask
   Parameter Request List Item: (3) Router
   Parameter Request List Item: (6) Domain Name Server
   Parameter Request List Item: (15) Domain Name
   Parameter Request List Item: (31) Perform Router Discover
   Parameter Request List Item: (33) Static Route
   Parameter Request List Item: (43) Vendor-Specific Information
   Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
   Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
   Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
   Parameter Request List Item: (119) Domain Search
   Parameter Request List Item: (121) Classless Static Route
   Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
   Parameter Request List Item: (252) Private/Proxy autodiscovery
```

#### 4.オプション77:ユーザクラス

ユーザクラスは、デフォルトでは最も一般的に使用されないオプションであり、クライアントを 手動で設定する必要があります。たとえば、Windowsマシンでこのオプションを設定するには、 ipconfig /setclassid "ADAPTER\_NAME" "USER\_CLASS\_STRING" アダプタ名は、コントロールパネルの[ネットワークと共有センター]で確認できます。



CMDでWindows 10クライアント用のDHCPオプション66を設定します(管理者権限が必要)。



Windowsのオプション66の実装により、Wiresharkはこのオプションをデコードできず、オプション66の後に来るパケットの一部が不正な形式として表示されます。

	✓ Option: (77) User Class Information
	Length: 15
	✓ Instance of User Class: [0]
	User Class Length: 116
۷	[Malformed Packet: DHCP/BOOTP]
	[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
	[Malformed Packet (Exception occurred)]
	[Severity level: Error]
	[Group: Malformed]

## HTTPプロファイリング

HTTPプロファイリングは、9800 WLCがサポートする最も高度なプロファイリング方法であり、 最も詳細なデバイス分類を提供します。

クライアントをHTTPプロファイルするには、「Run」状態にしてHTTP GET要求を実行する必要 があります。

WLCが要求を代行受信し、パケットのHTTPヘッダーの「User-Agent」フィールドを調べます。

このフィールドには、分類に使用できるワイヤレスクライアントに関する追加情報が含まれてい ます。

デフォルトでは、ほぼすべてのメーカーが、ワイヤレスクライアントがインターネット接続チェックを実行する機能を実装しています。

このチェックは、自動ゲストポータル検出にも使用されます。 デバイスがステータスコード 200(OK)のHTTP応答を受信した場合は、WLANがwebauthで保護されていないことを意味します その場合、WLCは残りの認証を実行するために必要な代行受信を実行します。 この最初のHTTP GETは、WLCがデバイスのプロファイリングに使用できる唯一のHTTP GETではありません。

後続のHTTP要求はすべてWLCによって検査され、さらに詳細な分類が行われる可能性がありま す。

Windows 10デバイスは、ドメイン**msftconnecttest.com**を使用してこのテストを実行します。 Appleデバイスは**captive.apple.com**を使用しますが、Androidデバイスは通常 **connectivitycheck.gstatic.com**を使用します。

このチェックを実行しているWindows 10クライアントのパケットキャプチャは次のとおりです。 [User Agent]フィールドに**Microsoft NCSI**が入力され、クライアントがWLC上で**Microsoft-Workstation**としてプロファイルされます。



HTTP経由でプロファイルされたクライアントのshow wireless client mac-address [MAC\_ADDR] detailedの出力例を次に示します。

Protocol	:	НТТР
Device OS	:	Windows NT 10.0; Win64; x64; rv:76.0
Protocol Map	:	0x000029 (OUI, DHCP, HTTP)
Device Name	:	MSFT 5.0
Device Type	:	Microsoft-Workstation

# RADIUSプロファイリング

デバイスの分類に使用される方法に関しては、ローカルとRADIUSのプロファイリングに違いは ありません。

Radiusプロファイリングが有効な場合、WLCはベンダー固有の特定のRADIUS属性セットを使用 してデバイスについて学習した情報をRADIUSサーバに転送します。

### DHCP RADIUSプロファイリング

DHCPプロファイリングによって取得された情報は、ベンダー固有のRADIUS AVPairとしてアカウンティング要求内のRADIUSサーバに送信されます cisco-av-pair:dhcp-option=<DHCP option>

DHCPオプション12、60、および55のAVPairsを示すアカウンティング要求パケットの例。 WLCからRADIUSサーバにそれぞれ送信されます(Wiresharkのデコードにより、オプション 55の値が破損している可能性があります)。

Bit 9, 199990         Bit 4, 17, 12         Bit 4, 17, 12         Bit 0, 19995         Bit 1, 19996         Bit 0, 19996         Bit 1, 19996 <th>ю.</th> <th>Time</th> <th>Source</th> <th>Destination</th> <th>Protocol</th> <th>Langth</th> <th>Source Part</th> <th>Destination Part</th> <th>24</th> <th></th>	ю.	Time	Source	Destination	Protocol	Langth	Source Part	Destination Part	24	
0         04.00         04.44.71.70         04.44.70.20         04.44.70.70         04.70 </td <td>14</td> <td>829 9,290998</td> <td>18.48.39.252</td> <td>38.48.73.92</td> <td>8400/5</td> <td>783</td> <td>64389</td> <td>1413</td> <td>Accounting-Request 1</td> <td>4-242</td>	14	829 9,290998	18.48.39.252	38.48.73.92	8400/5	783	64389	1413	Accounting-Request 1	4-242
000000         100.46.71.70         10.46.75.712         0.00000         42.101         0.0100         Accounting-Response 16-202, Duplinate Response           0         Prame 129; 703.5gtes on wire (12046 bits), 703.5gtes captured (1204 bits)	τ.	840 9.198995	10.48.71.92	10.48.39.212	840045	62	1813	64189	Accounting Response	6.6=282
<pre>c c c c c c c c c c c c c c c c c c c</pre>	L.	858 9.298995	10.48.71.92	18.48.39.212	BADDUS	6.2	1813	64189	Account Eng-Besponse	18-282, Duplicate Response
<pre>&gt; Prave #29: 783 hytes an wire (4244 hits), 783 hytes ceptured (4264 hits) &gt; Ethernet 12, 5x1 decelegieueee (exicutive)exicute(exicut)exicut)exicute(exicut)exicute(exicut)exicut) &gt; Sterret Yorkeesil Verbical Verbical (ALS.5.2.2) (but is.e.e.7.152) &gt; User batagree Protocol, 5x2 Pert (4128, 6x7 Pert is.e.7.152) &gt; User batagree Protocol, 5x2 Pert (4128, 6x7 Pert is.e. Mobile Protocol Code: Accounting-Report (4) Packet (berrifler: 4xx2 Pert (4128, 6x7 Pert is.e. Packet (berrifler: 4xx2 Pert is.e. Pa</pre>	<									
<pre>bit Next 121, 521 (000000000000000000000000000000000000</pre>	÷	from \$25. 203 holes	a on other (state bit	into the second second	OTHER DEPAY					
<pre>&gt; biterest big pill version a, big big version a, big big big big big big big big big big</pre>	0	Print and The Section	S OR WATE (Same of	to, no synth captures	(6254 8575)	100.00		and a		
<pre>&gt; defined frequency termine to find the definition of the final field &gt; where backgraph Protocols Code: Accounting-Respect (4) Packet Identifier: Base (30) Length: 34 Authoritizator: Jac2864as/Phil1200000055565 (The response to this respect is in free Add) &gt; Addr trivendor-Specific(3) 1+5 undering protocol() &gt; Whet trivendor-Specific(3) 1+5 undering protocol() &gt; Under 15 trivendor-Specific(3) 1+5 un</pre>	0	Tenernet say provide	station & Section 18			(				
<pre>vedeo stag we shall be to be a class of the total and total a</pre>	0	Data Batancas Bosto	cal for Burts 641	the floor Bourty 1813	- 74					
<pre>c decis fremedes Got Accounting-Request (A) Packet Seturiting-Request (A) Packet Seturiting</pre>	2	Adding Basharal	on, ser Pirti Ha	in, out parts said						
<pre>book incomparing wrights (v) packet Benifize in the (202) Length 34 activation is (2006cade?Net71005codeStric5 [Thm response to this response to the response to this response to this response to this response to the respo</pre>		Code: Accounting	demond (4)							
<pre>institute intervention intervention (intervention) institute intervention intervention institute intervention intervention institute ins</pre>		Backet Ldentidle	to design (367)							
<pre>authentics authentics authentics in the sequence is this response is in frame deal if not sequence is this response is the information if the sequence is the sequence is in the se</pre>		Length: 343	ci ente (see)							
<pre>The results and the field of the field</pre>		Authentication 1	CONTRACTOR NOTICE	A DOM NO. THE OWNER, NO. OF CO.						
<pre>v #tt://www.sec.in/scilic/actives/vtees/v) &gt; APP: tvvendor-3pecific/db 1=45 vnd=iscilytees/v) </pre>		The response to	this request is is	Frame 8491						
<pre>&gt; ##9: tvvendor-Specific(36) 1+8: vud=ticctpytees(9) &gt; vuder 12: (loidfytes (8) &gt; vuder 12: (loidfytes (8) &gt; vuder 12: (loidfytes (8) &gt; vuder 13: (loidfytes (8</pre>		w attribute value i	Pairs							
<pre>&gt; APF: tviendor-Specific(36) Exit underExceptions(0) &gt; APF: tviendor-Specific(36</pre>		) JUP: tollendor-	description to an	underEnergienteen(W)						
<pre>&gt; APP, Evender-Tpe:3Fi(36) b=0 vold-backpytee(0) &gt; Volder-Tp: 4 b Evender-Tp: 6 biologytee (0) &gt; Volder-Tp: 6 biologytee (0) &gt; Volder-Tp: 6 biologytee (0) &gt; APP, Evender-Tpe:3Fi(26) b=0 vold-backpytee(0) </pre>		) JUP: Extendor	Specific(26) 1+10	under Excellenteen (9)						
<pre>&gt; MM% Evender-Specific(28) 1-30 vnd=licit/ystem(1) &gt; MM% Evender-Specific(28) 1-30 vnd=licit/ystem(1) &gt; MM% Evender-Specific(28) 1-30 vnd=licit/ystem(1) * MM% Evender-Specific(28) 1-30 vnd=licit/ystem(1) * ystafe 28: (Licit/ystem (2) * Vnder 28: (Licit/ystem (2) * Vnder 28: (Licit/ystem (3) * Vnder 2</pre>		) JUP: Ervendor-	Specific(26) bell	under Lauritystees (9)						
<pre>&gt; MM1 Torvendor-Specific(36) 1+30 vold-ticcofysteme(9) &gt; MM2 torvendor-Specific(36) 1+30 vold-ticcofysteme(9) * WM1 torvendor-Specific(36) 1-30 vold-ticcofysteme(9) * Dors torvendor-Specific(36) 1-30 vold-ticcofysteme(9) * Vendor 28 (Locofystem (8) * Wendor 28 (Locofystem (8)) * Wendor 28 (Locofys</pre>		> ave: p-vendor-	-teeclific(26) 1-be	under Lacobysteen (9)						
<pre>&gt; WM% tweedor-Specific(26) 1-35 web-class/pites(9) &gt; WM% tweedor-Specific(26) 1-35 web-class/pites(9) Tppe: 26 Length: 39 Web-class(ListOpytes(9) &gt; VSA: t-Class-mMale(1) 1-33 web-decp-option-1000(F00004012056F00-4L0000K) * Web-class(ListOpytes(9) * VSA: t-Class-mMale(1) 1-32 web-class/pites(9) * VsA: t-Class-mMale(1) 1-32 web-class/pites(1) * VsA: t-Class-mMa</pre>		WP: D-Vendor-	-Specific(26) 1-50	und-classifystees(b)						
<pre>&gt; WW: twiender-Specific(36) 1+39 vml+claceSystem(9) Type: 24 Longth: 39 Vmlder 20: (LocSystems (8) Vmlder 20: (LocSystems (8) Type: 24 Longth: 32 Vmlder 20: (LocSystems (8) Vmlde</pre>		> AVP: t-Vendor-	description 1-15	und-classfurtees(9)						
Type: 24         Length: 25         Vender 25: (Loidlystee: (%)         Vender 25: (Loidlystee: (%)         * Will: (-State-while(): Loid vender(backbar)         * Winder 25: (Loidlystee: (%)		w July: Evidender-	descification 1+89	undeclassfuntees(N)						
<pre>(ength: 3P Vender 2D: (dointystee.(%) &gt; Volt: R=Cleve-anter(%) ==32 vel-dog-option=laber(footal2005x10=-culture. &gt; NP: R=Cleve-anter(%) ==32 vel-dog-option=laber(footal2005x10=-culture. &gt; NP: R=Cleve-anter(%) ==32 vel-dog-option=laber(sectors)=1.5,8 &gt; Vender 2D: (dointystee.(%) &gt; Vender 2D: (dointystee.(%) &gt; NP: R=Vender-Specific(20) 1=32 vel-dog-option=laber(sectors)=1.5,8 &gt; NP: R=Vender-Specific(20) 1=32 vel-dog-option=laber(sectors)=1.5,8 &gt; NP: R=Vender-Specific(20) 1=32 vel-dog-option=laber(sectors)=1.5,8 &gt; NP: R=Vender-Specific(20) 1=32 vel-dog-option=laber(sectors)=1.5,8 &gt; Vender 2D: (dointystee.(%) &gt; Vend</pre>		Type: 26								
Verdie: 20: (SciOpytems (9)           Void: t-Clicce-servic(1):1-33 velocity-option-indep:Protect201501501-01-01.000000           Point t-Verdie: Servic(1):1-33 velocity-option-indep:Protect201501501-01-01.000000           Point t-Verdie: Servic(1):1-32 velocity-option-indep:Protect201501501-01-01.000000           Verdie: Tot (SciOpytems (8)		Longth: 39								
<pre>&gt; VAL 1<state=ava(()) 3-33="" val="decp=option=10001F00F10150510F-statemx"> Web: twendor-Specific(20) 1-52 val=tbcctytees(0) F(port 26 Length: 32 Vender-Specific(20) 1-52 val=tbcctytees(0) Vender-Specific(20) 1-52 val=tbcctytees(0) F(port 26 Length: 36 Vender-Specific(20) 1-52 val=tbcctytees(0) F(port 26 Vender-Spe</state=ava(())></pre>		Vendor 101	cloudystees (9)							
<pre>wdf: twwedor-Specific(28) 1+32 vmd=class/systems(8) Type: 26 Langth: 32 Vender 28: class/systems (8) Vender 28: class/systems(8) Type: 26 Langth: 38 Vender 28: class/systems(8) Type: 26 Langth: 38 Vender 28: class/systems(8) Type: 26 Langth: 38 Vender 28: class/systems(8) Vender 28: class/systems(8) Vender 28: class/systems(8) Vender 28: class/systems(8) Vender 28: class/systems(8)</pre>		> VEAL CHOICE	00-00Pale(1) 3+33 v	ab-dhop-option=\abbi\f\ab	MP-REPORTATION-READ	erus.				
Type: 26       Langth: 32       Vendor: 30: closeSystems (N)       Vendor: 50: closeSystems (N)       WM: twendor: 50: closeSystems (N)       Vendor: 50: closeSystems (N)       Vendor: 10: closeSystems (N)		w AvP: t-Vendor-	-Specific(26) 1+52	und-clocatystees(9)		_				
<pre>(ength: 32 Vender 10: closofystems (8) vedar t-Closom whe(cl) 1-28 web-closofystem(8) vedar t-Closom whe(cl) 1-28 web-closofystem(8) vedar t-Closofystems (8) vedar t-Closofystems (8) vedar t-Closofystems (8) vedar t-Closofystems (8)</pre>		Type: 26								
Vender 18: (Scrötystens (8) V MAR HS Scrothwich(3) 2-01 with the constraints (2001/001/01/27.5.0) W MAR HS Scrothwich(3) 2-01 with the constraints (2001/001/01/27.5.0) Pyper 20 Pyper 20 Length(3) Vender 18: clochystens (8) Vender 18: clochystens (9) Vender 18: clochystens (9)		Longth: 32								
(x) VAAL 145 (associated (x) and a second constant (associated (x))     (x) Verender-Specific (20) 1-20 verender(20)     (y) verender-Specific (20) 1-20 verender(20)     (y) verender-Specific (x) Verender(20)     (x) Verender(20) Verender(20)     (x) Verender(20) Verender(20)		Vendor 301	closedystees (9)							
WM: Kvender-Specific(28) 1-38 vnd=classbysteec(9) Type: 26 Length: 38 Vender 18: classbysteec (9) Vender 18: classbysteec (9)		<ul> <li>MAX AND A</li> </ul>	terminateriti beze n	Contract of Conversion Conversion	Carden S.A					
Type: 26 Length: 36 Vendor 10: clocofystems (9) • VSA: t=Cloco-AVM(r(s) 1-3) vs3=drcp-option=100070001000100010001000100010001000100		* AVP: E-Vendor-	-tpec1754(28) 3+38	ved-classifystees(9)						
Length: 38 Vendor 38: closofystem: (8) > Vsk: t-(1:co-meta(r(s) 1-s) val-docp-option-laber/abs/des/des/des/des/des/des/des/des/des/de		Type: 26								
Vendor 10: clocofystems (0)  Vdar t=(isco-wena(r(s) 1-0) val-decp-option=laser/assister/ass		Length: 38								
VSA: t=Cscc=WHa(r(s) 3+52 valuebup-option=100010001000100010010010010010010010010		Vendor 181	cinceSystems (9)					-		
		In VSAU THESE	on-Aven(1) 1+52 v	al-dicp-option-lateriae	FUELDER MEDITALES VALUES	127-012	The section in the			

# HTTP RADIUSプロファイリング

HTTPプロファイリング(HTTP GET要求のヘッダーのUser-Agentフィールド)によって取得さ れた情報は、ベンダー固有のRADIUS AVPairとしてアカウンティング要求内のRADIUSサーバに 送信されます cisco-av-pair:http-tlv=User-Agent=<user-agent>

初期接続チェックHTTP GETパケットには、User-Agentフィールドに多くの情報が含まれず、「 Microsoft NCSI」のみが含まれます。この単純な値をRADIUSサーバに転送するアカウンティング パケットの例を示します。

4047 3583,868996	38.48.39.212	58.48.71.92	8400V5	708 57397	1813	Accounting-Request 58-385
4854 3583,875888	38.48.71.92	58.48.39.212	8400V5	62 1813	57397	Accounting-Response id-105
4855 3583.875988	38.48.71.92	10.48.39.212	R403V5	62 1813	57397	Accounting-Response id-105, Duplicate Response
User Datagram Proto	cel, Sec Ports 577	HO, Dot Port: 1813				
MODUS Presecel						
Code: Accounting	-Request (4)					
Packet Identifie	ri 8x69 (105)					
Length: 658						
AuthentLiators 8	00640-0736-434649	0683879661244				
[The response to	this report is i	a frame appal				
w Attribute value	Pales					
> JUP: ErVendor	-Sam(D/L((28)) 2+64	ved-classifystees(9)				
> auto township	-Specific(26) 2+07	underLocationtees(9)				
> auto township	-Specific(26) 2+68	ved-closedystees(9)				
> suf-c t-vendor	-SpecI/Lc(26) 5+28	underLocativations(9)				
> AVP: E-Vendor	-SpecI/Lc(26) 2+08	ved-closedystees(9)				
> AVP: E-yendor	-tae(1/L((24) 3-21	under Location Leng (95				
W July: E-Vendor	-Spect/Lc(26) 5-01	und-closedustees(9)				
Type: 26						
Length: 35						
Vendor ID:	classifystees (9)					
> VSAL D-CEA	co-Auffwir(1) 1+29	val-http-t3v-\800\800'	analysis microsoft	8010		

ユーザがインターネットの閲覧を開始し、追加のHTTP GET要求を作成すると、インターネット に関する詳細情報を取得できます。

WLCは、このクライアントの新しいユーザエージェント値を検出すると、追加のアカウンティン グパケットをISEに送信します。

この例では、クライアントがWindows 10 64ビットとFirefox 76を使用していることを確認できます。

47	44 3595.102000	38.48.39.212	38.48.71.92	RADOV5	765 57397	1813	Accounting-Request id+106
42	49 3595.111994	38.48.71.92	38.48.39.232	RADOV5	62 1813	\$7397	Accounting-Response 1d=386
47	58 3595.111994	38.48.71.92	38.48.39.212	RADOV5	62 1813	\$7397	Accounting-Response id=386, Duplicate Response
üse	Datagram Proto	cel, Src Port: 577	97, Dot Port: 1813				
B.AQ	US Protocol						
-	oder: Accounting	-Request (4)					
	acket identifie	r: 8x6a (106)					
1	ength: 729						
	uthenticator: 4	dild5c3dibileeae7di2	45807F9844f2f				
	The response to	this report is i	n frane (269)				
~ <b>)</b>	ttribute Value I	Palins					
	AVP: t-Vendor	-Specific(26) 1+44	vml+claceSystems(9)				
	AVP: t-Vendor	-Specific(26) 1+07	vn8+cEsce5ystems(9)				
	#VP: t+Vendor	-Specific(26) 1+48	vml+claceSystems(9)				
	#VP: t-Vendor	-Specific(26) 1+29	vnd+cEscoSystems(9)				
	#VP: t-Vendor	-Specific(26) 1+38	vnd+cEscoSystems(9)				
	WP: twVendor	<specific(26) 1+26<="" td=""><td>vnd+cEscoSystems(9)</td><td></td><td></td><td></td><td></td></specific(26)>	vnd+cEscoSystems(9)				
	#VP: t-Vendor-	-Specific(26) 1+99	vm8+cEscoSystems(9)				
	Type: 26						
	Length: 99						
	Vendor 10:	clacoSystems (9)					
	> VSA: t+Cin	co-AsPair(1) 1+95	val-http-tlv=\000\001	abbrecills/5.0	Windows NT 18.8; W	0464; x64; rv	(76.4) Gecko/200000181 /Srefex/76.4

# 9800 WLCでのプロファイリングの設定

# ローカルプロファイリング設定

ローカルプロファイリングを機能させるには、[Configuration] > [Wireless] > [Wireless Global]で [Device Classification]を有効にします。このオプションは、MAC OUI、HTTP、およびDHCPプロ ファイリングを同時に有効にします。

Configuration \* > Wireless \* > Wireless Global

Default Mobility Domain *	default	<u>+</u>
RF Group Name*	default	
Maximum Login Sessions Per User*	0	
Management Via Wireless		
Device Classification		
AP LAG Mode		

また、[Policy configuration]で、[HTTP TLV Caching]と[DHCP TLV Caching]を有効にできます。 WLCは、プロファイルがない場合でもプロファイリングを実行します。

これらのオプションを有効にすると、WLCはこのクライアントに関して以前に学習した情報をキ

ャッシュし、このデバイスによって生成された追加のパケットを検査する必要がなくなります。

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	BlockPoli	cy x v	

## RADIUSプロファイリングの設定

RADIUSプロファイリングが機能するためには、(「ローカルプロファイリングの設定」で説明 したように)デバイス分類をグローバルに有効にする以外に、次の作業が必要です。

1. RADIUSサーバを指す「ID」タイプを使用して、AAAアカウンティング方式を設定します。

Configuration * >	Security* > AAA						
+ AAA Woord							
Servers / Groups	AAA Method List	AA Advanced					
Authentication Authorization	+ A55	× Delete					
Accounting	Name	< Type	< Group1	< Group2	< Group3	< Group4	~
	AccMethod	identity.	15622	NIA	NA	NA	
	A 4 1	H 20 .	itoms per page			1 - 1 d	1 itema

2. [Configuration] > [**Tags & Profiles] > [Policy] > [Policy\_Name] > [Advanced]でアカウンティング** 方式を追加する必要があります。

dit Policy	y Profile				
eneral	Access Policies	QOS and AVC	Mobility	Advanced	
WLAN T	ïmeout			Fabric Profile	
Session 1	limeout (sec)	1800		mDNS Service Policy	default-mdns-servic
die Time	out (sec)	300			Country Colors
die Thre	shold (bytes)	0		Hotspot Server	Search or Select
Client Ex	clusion Timeout (sec)	60		User Private Netwo	rk
Guest LA	N Session Timeout	0		Status	
DHCP		_		Drop Unicast	
	10 December 1			Umbrella	
DHCP Se	rver IP Address			Umbrella Parameter Map	Not Configured
w more				Flex DHCP Option for DNS	ENABLED
VAA Po	licy			DNS Traffic Redirect	IGNORE
Now AA	A Override			WLAN Flex Policy	
NAC Stat	0			VLAN Central Switchi	ng 🔲
VAC Typ	0	RADIUS	•	Solt MAC ACL	Search or Select
Policy Na	me	default-aaa-policy	* *		
Accounti	ng List	AcctMethod	× •	Air Time Fairness P	olicies

3.最後に、[Configuration] > [Tags & Profiles] > [Policy]で[RADIUS Profiling]チェックボックスをオ ンにする必要があります。このチェックボックスは、HTTPとDHCPの両方のRADIUSプロファイ リングを有効にします(古いAireOS WLCには2つの個別のチェックボックスがありました)。

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	BlockPoli	cy x v	

# プロファイリングの使用例

### ローカルプロファイリング分類に基づくローカルポリシーの適用

この設定例では、Windows-Workstationとしてプロファイリングされたデバイスだけに適用され る、YouTubeおよびFacebookアクセスをブロックするQoSプロファイルを使用したローカルポリ シーの設定を示します。

わずかな変更を加えると、この設定を変更して、たとえばワイヤレス電話だけに特定のDSCPマ ーキングを設定できます。

[Configuration] > [Services] > [QoS] に移動して、QoSプロファイルを作成します。[add]をクリッ クして新しいポリシーを作成します。

Cisco Cat	ilyst 9800-CL Wireless Controller	Welcome admin		Q.
Q. Search Maria Sama	Configuration * > Services * > QoS			
Dashboard	· Add			Double AutoColl
(a) Monitoring	Polcy Name - Associated Class-Maps		<ul> <li>Associated Interfaces/Profiles</li> </ul>	
🗞 Configuration 💦 🔸	· · · · · · · · · · · Intern per page			No issues to display

ポリシー名を指定し、新しいクラスマップを追加します。使用可能なプロトコルから、ブロック する必要があるプロトコル、DSCPがマークされているプロトコル、または帯域幅が制限されて いるプロトコルを選択します。

この例では、YouTubeとFacebookがブロックされています。QoSウィンドウの下部にあるPolicy Profilesには、このQoSプロファイルが<u>適用されないことを確認してください</u>。

QoS		
Auto QOS	DISABLED	
Policy Name*	block	
Description		
Match v Match Type Value	Mark v. Mark v. Police Value v. Drop v. Drop v. Defined AVC/User v. Actions	~
н 4 0 н н	20 • Items per page No items to dispi	lay
	× Deleta	
AVC/User Defined	AVC • @Any O All	
Drop		
Match Type	protocol v	
	Available Protocol(s) Selected Protocol(s)	
	3com-amp3 3com-tsmux 3pc 4chan v ≪	
	2 Carrol Save	

Available (8)			Selected (0)		
Profiles			Profiles	Ingress	Egress
🛜 vasa	+	î			
🛜 33nps	÷				
🛜 webauth	*				
😭 11Iwebauth	*				
11mobility	+				
11override	+				
				_	_
Dancel					🗎 Apply to De

[Configuration] > [Security] > [Local Policy] に移動し、新しいサービステンプレートを作成します

Configuration * > Security * > Local Policy		
Service Template Policy Map		
+ Add X Delete		
Service Template Name	< Source	~
webauth-global-inactive		
DIFAUT_ORTICAL_DATA_TEMPLATE		
DIFAULT_ORTICAL_VOICE_TEMPLATE		
DEFAULT_LINKSEC_POUCY_MUST_SECURE		
DEFAULT_LINKSEC_POUCY_SHOULD_SECURE		
H + 1 + H 20 • Tamo per page		1 - 5 of 5 items

o

前の手順で作成した入力および出力QoSプロファイルを指定します。この手順では、アクセスリ ストも適用できます。VLANを変更する必要がない場合は、vlanフィールドを空のままにします。

Create Service Template		×
Service Template Name*	BlockTemplate	
VLAN ID	1-4094	
Session Timeout (secs)	1-65535	
Access Control List	None	•
Ingress QOS	block x	
Egress QOS	block x	•
mDNS Service Policy	Search or Select	· Î
Cancel		Apply to Device

#### [Policy Map]タブに移動し、[add]をクリックします。

Configuration * > Security * > Local Policy	
Service Template Policy Map	
+ Add × Delete	
Policy Map Name	~
BULTIN, AUTOCONF, POLICY	
H + 1 + H 20 • Tarms per page	1 - 1 of 1 itoms

ポリシーマップ名を設定し、新しい基準を追加します。前の手順で作成したサービステンプレートを指定し、このテンプレートを適用するデバイスタイプを選択します。

この場合、Microsoft-Workstationが使用されます。複数のポリシーが定義されている場合は、最 初の一致が使用されます。

もう1つの一般的な使用例は、OUIベースの一致基準を指定することです。導入環境に同じモデル のスキャナまたはプリンタが多数存在する場合、通常は同じMAC OUIを使用します。

これは、特定のQoS DSCPマーキングまたはACLを適用するために使用できます。

olicy Map Name *	BlockPolicy	
latch Criteria List		
+ Add X Dev	te Move To ANVe Up Move Down	
Device Type(Match Criteria)	✓ User Role(Match v User Name(Match v OUI(Match v Address(Match v Address(Match v Address(Match oriteria) Service Temp	ninte -
dd Match Criteria	20 • terms per page No terms t BlockTemplate x •	to display
k + 0 + K add Match Criteria ervice Template * evice Type	20 • terms per page No terms 1 BlockTemplate • Microsoft-Workstatic •	o display
evice Type ser Role	20 • terms per page No terms of BlockTemplate • • eq • Microsoft-Workstadd • Select Fiber Type • Enter User Role	to display
envice Template * envice Type ser Role	20 • terms per page No terms of ElockTemplate • • eq • Microsoft-Workstadd • Select Fiber Type • Enter User Role Select Fiber Type • Enter User Name	to display
evice Type ser Name	20 • terms per page       No terms to         BlockTemplate • •       •         eq • • Microsoft-Workstade •       •         Select Fiber Type • • Enter User Role       •         Select Fiber Type • • Enter User Name       •         Select Fiber Type • • • Enter User Name       •         Select Fiber Type • • • • • • • • • • • • • • • • • • •	to display

WLCがYouTubeおよびFacebookトラフィックを認識できるようにするには、アプリケーションの可視性をオンにする必要があります。

[Configuration] > [Services] > [Application Visibility] に移動します。wlanのポリシープロファイルの可視性を有効にします。

inguination of Derivors 1	<ul> <li>Application Visibilit</li> </ul>	la l			
Definition of the second secon	ine Policy Invarit Interart Interart				
rag and Drop, double click or o Available (11)	lick on the button from S	elected Profiles to addiremove Profi	les	Q. Search	Ei Appiy
		Beating .	Maihiller	Automatic Littlener	
Profiles		PTOTHES	Amouth	Collector Address	
Profiles	+ 1	11ovenide	(all all all all all all all all all all	Local 🖉 External	+
Trofiles	*	11ovenide	(c)	Local 🖉 Edemai	+
Profiles           11hrebauth           11mobility           11mobility           11profiling	*	Tovende	(and	Local Ø Desmai	٠
hotes illeobauth illeobauth illeobaity illeo	* * *	Toveride		Local / Ddemai	*
Profiles  11hrebauth  11hrobity  11profiling  33nps  Capwap1	* * * * * * *	11ovenide	(and a second	Local 🖉 Désmal	+

ポリシープロファイルで[HTTP TLV Caching]、[DHCP TLV Caching]、[Global device Classification]が有効になっており、ローカルサブスクライバポリシーが、前のいずれかの手順で 作成されたローカルポリシーマップを指していることを確認します。

fit Polic	y Profile						
eneral	Access Policies	QOS and AVC	Mobility	Advanced			
RADIUS	Profiling				WLAN ACL		
HTTP TL	V Caching				IPv4 ACL	Search or Select	•
DHCP TL	V Caching				IPv6 ACL	Search or Select	•
WLANI	ocal Profiling				URL Filters		
Global S Classifica	tate of Device ation	Enabled (	D		Pre Auth	Search or Select	•
Local Su	bscriber Policy Name	BlockPol	icy x •	]	Post Auth	Search or Select	•
VLAN							
VLAN/VL	AN Group	VLANOO	39 •	)			
Multicast	VLAN	Enter M	ulticast VLAN	1			

クライアントが接続すると、ローカルポリシーが適用されているかどうかを確認し、YouTubeと Facebookが実際にブロックされているかどうかをテストできます。

show wireless client mac-address [MAC\_ADDR] detailedの出力には、次が含まれます。

```
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	:	<pre>wlan_svc_1loverride_local (priority 254)</pre>
VLAN	:	VLAN0039
Absolute-Timer	:	1800
Device Type :	M	licrosoft-Workstation
Device Name :	M	SFT 5.0
Protocol Map :	0	x000029 (OUI, DHCP, HTTP)
Protocol :	н	TTP

### Cisco ISEの高度なポリシーセットのRADIUSプロファイリング

RADIUSプロファイリングを有効にすると、WLCはプロファイリング情報をISEに転送します。 この情報に基づいて、高度な認証および許可ルールを作成できます。

この記事では、ISEの設定については説明しません。詳細については、『<u>Cisco ISEプロファイリ</u> <u>ング設計ガイド</u>』を参照してください。

このワークフローでは通常、CoAを使用する必要があるため、9800 WLCでCoAが有効になって いることを確認してください。

# FlexConnectの導入におけるプロファイリング

## 中央認証、ローカル スイッチング

この設定では、ローカルとRADIUSの両方のプロファイリングが、前の章で説明したとおりに動作し続けます。APがスタンドアロンモードになると(APがWLCへの接続を失うと)、デバイスのプロファイリングは機能しなくなり、新しいクライアントは接続できなくなります。

### ローカル認証、ローカル スイッチング

APが接続モード(APがWLCに加入)の場合、プロファイリングは引き続き動作します(APはク ライアントDHCPパケットのコピーをWLCに送信して、プロファイリングプロセスを実行します )。

プロファイリングが機能しても、認証はAP上でローカルに実行されるため、プロファイリング情報をローカルポリシー設定やRADIUSプロファイリングルールに使用することはできません。

# トラブルシューティング

#### 放射能痕跡

WLCでクライアントプロファイリングをトラブルシューティングする最も簡単な方法は、放射性 トレースを使用することです。[Troubleshooting] > [Radioactive Trace] に移動し、クライアント ワイヤレスアダプタのMACアドレスを入力して、[Start] をクリックします。

#### Troubleshooting > Radioactive Trace

Co	nditional Debug Global Stat	e: Started	
+	Add × Delete	Start Stop	
	MAC/IP Address	Trace file	
	74da.38f6.76f0	debugTrace_74da.38f6.76f0.txt 📥	► Generate
14	< 1 ⊨ ⊨ 20	<ul> <li>items per page</li> </ul>	1 - 1 of 1 items

クライアントをネットワークに接続し、実行状態になるまで待ちます。トレースを停止し、 Generateをクリックします。[Internal Logs]が有効になっていることを確認します(このオプショ ンは17.1.1リリース以降にのみ存在します)。

Enter time interval		×
Enable Internal Logs		
Generate logs for last	10 minutes	
	O 30 minutes	
	O 1 hour	
	<ul> <li>since last boot</li> </ul>	
	O 0-4294967295 seconds v	
	Ū	
Cancel	Apply to Device	

#### 以下に、放射性物質の痕跡から得られた関連する断片を示す:

WLCによってMicrosoft-Workstationとしてプロファイルされるクライアント:

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

#### デバイス分類をキャッシュする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 キャッシュ内のデバイス分類を検出するWLC:

(info): [74da.38f6.76f0:capwap\_90000004] Device type found in cache Microsoft-Workstation 分類に基づいてローカルポリシーを適用するWLC:

(info): device-type filter: Microsoft-Workstation required, Microsoft-Workstation set - match for 74da.38f6.76f0 / 0x9700001A (info): device-type Filter evaluation succeeded (debug): match device-type eq "Microsoft-Workstation" :success DHCPおよびHTTPプロファイリング属性を含むアカウンティングパケットを送信するWLC:

[caaa-acct] [21168]: (debug): [CAAA:ACCT:c9000021] Accounting session created [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap\_90000004] Getting active filter list [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap\_90000004] Found http [auth-mgr] [21168]: (info): [74da.38f6.76f0:capwap\_90000004] Found dhcp [aaa-attr-inf] [21168]: (debug): Filter list http-tlv 0 [aaa-attr-inf] [21168]: (debug): Filter list dhcp-option 0

[aaa-attr-inf] [21168]: (debug): Get acct attrs dc-profile-name 0 "Microsoft-Workstation" [aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-name 0 "MSFT 5.0" [aaa-attr-inf] [21168]: (debug): Get acct attrs dc-device-class-tag 0 "Workstation:Microsoft-Workstation" [aaa-attr-inf] [21168]: (debug): Get acct attrs dc-certainty-metric 0 10 (0xa) [aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 0c 00 0f 44 45 53 4b 54 4f 50 2d 4b 4c 52 45 30 4d 41 [aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 3c 00 08 4d 53 46 54 20 35 2e 30 [aaa-attr-inf] [21168]: (debug): Get acct attrs dhcp-option 0 00 37 00 0e 01 03 06 0f 1f 21 2b 2c 2e 2f 77 79 f9 fc

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

### パケット キャプチャ

中央でスイッチされる展開では、パケットキャプチャはWLC自体で実行できます。 [Troubleshooting] > [Packet Capture] に移動し、このクライアントが使用しているインターフェイ スの1つに新しいキャプチャポイントを作成します。

VLANでキャプチャを実行するには、VLAN上にSVIが必要です。SVIが存在しない場合は、物理ポ ート自体でキャプチャを実行します

Troubleshooting * > Packet Capture	
AAT NOT DOOR	
Capture - Name - Interface - Monitor Control Plane - Buffer Scie - Filter by - Limit Status	+ Actor
x x 0 x x 20 + term per page	
Create Packet Capture *	1
Capture Name* Depture	
Filter* #vy +	
Monitor Control Plane	
Buffer Size (M8)* 10	
Limit by* Duration v 3600 secs -+ 1.00 hour	
Available (4) Selected (1)	
🗑 ügabitihemet 1 🔶 🗑 Van39 +	
Ggebitherred +	
C Gastilleened +	
Van1 +	
To Cancel	

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。