Introduction

This article provides an in-depth look into how device classification and profiling works on Cisco Catalyst 9800 Wireless LAN Controllers, describes potential use cases, configuration examples and steps necessary to troubleshoot it.

Components Used

- 9800 CL WLC running 17.2.1 image
- 1815i Access Point
- Windows 10 Pro Wireless Client
- Cisco ISE 2.7

Profiling Process
Device profiling is a feature that offers a way to find out additional info about a wireless client that has joined the wireless infrastructure. Once device profiling is performed, it can be used to apply different local policies or to match specific RADIUS server rules.

Cisco 9800 WLCs are capable of performing 3 types of device profiling:

1. MAC address OUI
2. DHCP
3. HTTP

**MAC Address OUI Profiling**

MAC address is a unique identifier of each wireless (and wired) network interface. It is a 48-bit number usually written down in a hexadecimal format MM:MM:MM:SS:SS:SS. First 24 bits (or 3 octets) are known as OUI (Organizationally Unique Identifier) and they uniquely identify a vendor or manufacturer. They are purchased from and assigned by the IEEE. One vendor or manufacturer can purchase multiple OUIs.

Example:

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

Once a wireless client associates to the access point, the WLC performs the OUI lookup to determine the manufacturer. In Flexconnect local switching deployments, the AP still relays relevant client information to the WLC (like DHCP packets and client mac address)

Profiling based only on OUI is extremely limited and it might be able to classify device as a specific brand, but it will not be able to differentiate between a laptop and smartphone.

**Locally Administered MAC Addresses Issues**

Due to privacy concerns, many manufacturers started implementing mac randomization features into their devices. Locally administered MAC addresses are randomly generated and have a second-least-significant bit of the first octet of the address set to 1. This bit acts as a flag that announces that the mac address is actually a randomly generated one. There are four possible formats of locally administered MAC addresses (x can be any hex value):

- 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 devices by default uses a randomly generated locally administered MAC address each time they connect to a new SSID network. This feature completely defeats the OUI based device classification as the controller recognizes that the address has been randomized and does not perform any lookup.

**DHCP Profiling**

DHCP profiling is performed by WLC by looking into the DHCP packets wireless client is sending
out. If DHCP profiling was used to classify the device, the output of `show wireless client mac-address [MAC_ADDR] detailed` command will contain:

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

WLC will inspects several DHCP Option fields in the packets sent out by wireless clients:

1. Option 12 - Hostname

This option represents clients hostname and it can be found in the DHCP Discover and DHCP Request packets:

```
Option: (12) Host Name
    Length: 15
    Host Name: DFSK0P-KLREBA1
```

2. Option 60 - Vendor Class Identifier

This option is also found in the DHCP Discover and Request packets. With this option, clients can identify themselves to the DHCP server and the servers can then be configured to only respond to the clients with specific vendor class identifier. This option is most commonly used to identify the access points in the network and only respond to them with the option 43.

Examples of Vendor Class Identifiers

- “MSFT 5.0” for all Windows 2000 clients (and up)
- “MSFT 98” for all Windows 98 and Me clients
- “MSFT” for all Windows 98, Me and 2000 clients

Apple MacBook devices do not send out Option 60 by default.

Example packet capture from Windows 10 client:
3. Option 55 - Parameter Request List

DHCP Parameter Request List option contains configuration parameters (option codes) that the DHCP client is requesting from the DHCP server. It is a string written in comma separated notation (for example 1,15,43). Based

It is not a perfect solution because the data it produces is vendor-dependent and can be duplicated by multiple device types. For example, Windows 10 devices always by default request a certain parameter list. Apple iPhones and iPads use different set of parameters on which it is possible to classify them.

Example capture from Windows 10 client:

4. Option 77 - User Class

User class is an option that is most commonly not used by default and requires the client to be manually configured. For example, this option can be configured on a windows machine using the command:

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

Adapter name can be found in the Network & Sharing Center in control panel:
Configuring DHCP option 66 for Windows 10 client in CMD (requires administrator rights):

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

Due to Windows’ implementation of option 66, wireshark is not able to decode this option and part of the packet coming after option 66 shows up as malformed:

```
 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]
```

**HTTP Profiling**

HTTP profiling is the most advanced way of profiling 9800 WLC supports and it offers the most detailed device classification. In order for a client to be HTTP profiled, it needs to be in a “Run” state and perform an HTTP GET request. WLC will intercept the request and look into the “User-Agent” field in HTTP header of the packet. This field will contain additional information about the wireless client that can be used to classify it.

By default, almost all manufacturers have implemented a feature where a wireless client will try to perform internet connectivity check. This check is also used for automatic guest portal detection. If a device receives an HTTP response with status code 200 (OK), that means the WLAN is not secured with webauth. If it is, the WLC will then perform interception necessary to perform the rest of the authentication. This initial HTTP GET is not the only one WLC can use to profile the device. Every subsequent HTTP request is inspected by the WLC and it might result with even more detailed classification.

Windows 10 devices use the domain [msftconnecttest.com](http://msftconnecttest.com) to perform this test. Apple devices use [captive.apple.com](http://captive.apple.com), while Android devices usually use [connectivitycheck.gstatic.com](http://connectivitycheck.gstatic.com).
Packet captures of the Windows 10 client performing this check can be found below. The User Agent field is populated with Microsoft NCSI, which results in client being profiled on the WLC as Microsoft-Workstation:

Example output of `show wireless client mac-address [MAC_ADDR] detailed` for a client that is profiled 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
```

**RADIUS Profiling**

When it comes to methods used to classify the device, there is no difference between Local and RADIUS profiling. If Radius profiling is enabled, the WLC will simply forward the information it learned about the device through a specific set of vendor specific RADIUS attributes to the RADIUS server.

**DHCP RADIUS Profiling**

Information obtained through DHCP profiling is sent over to the RADIUS server inside the accounting request as a vendor-specific RADIUS AVPair `cisco-av-pair: dhcp-option=<DHCP option>`

Example of an accounting request packet showing AVPairs for DHCP option 12, 60 and 55, respectively sent from WLC to RADIUS server (option 55 value might appear as corrupted due to Wireshark's decoding):
HTTP RADIUS Profiling

Information obtained through HTTP profiling (User-Agent field from the header of HTTP GET request) will be sent over to the RADIUS server inside the accounting request as a vendor specific RADIUS AVPair cisco-av-pair: http-tlv=User-Agent=<user-agent>

Initial connectivity check HTTP GET packet does not contain much information in the User-Agent field, only "Microsoft NCSI". Example of an accounting packet forwarding this simple value to RADIUS server:

Once the user starts browsing the internet and creates some additional HTTP GET requests, it is possible to gain more information about it. WLC will send additional accounting packet to the ISE if it detects new User-Agent values for this client. In this example, it's possible to see that the client is using Windows 10 64 bit and Firefox 76:
Configuring Profiling on 9800 WLC

Local Profiling Configuration

In order for Local profiling to work, simply enable Device Classification under Configuration > Wireless > Wireless Global. This option enables MAC OUI, HTTP and DHCP profiling at the same time:

Additionally, under Policy configuration you can enable HTTP TLV Caching and DHCP TLV
Caching. WLC will still perform profiling if without them. With these options enabled, the WLC will cache previously learned information about this client and avoid having to inspect additional packets generated by this device.

### RADIUS Profiling Configuration

In order for RADIUS profiling to work, besides globally enabling device classification (like mentioned in Local Profiling configuration), it’s necessary to:

1. Configure AAA Accounting method with type “identity” pointing towards the RADIUS server:

   ![Configuration]

   ![AAA Method List]

   2. Accounting method needs to be added under Configuration > Tags & Profiles > Policy > [Policy_Name] > Advanced:
3. Finally, RADIUS Profiling checkbox needs to be ticked under Configuration > Tags & Profiles > Policy. This checkbox enables both HTTP and DHCP RADIUS profiling (old AireOS WLCs had 2 separate checkboxes):
Profiling Use Cases

Applying Local Policies Based on Local Profiling Classification

This sample configuration demonstrates configuration of Local Policy with QoS profile blocking youtube and facebook access that is applied only to devices profiled as Windows-Workstation. With slight changes, this configuration can be modified to, for example, set specific DSCP marking for only wireless phones.

Create a QoS profile by navigating to **Configuration > Services > QoS**. Click add to create new policy:

Specify the policy name and add a new class map. From the available protocols, select the ones that need to be blocked, DSCP marked or bandwidth limited. In this example, youtube and facebook will be blocked. Make sure not to apply this QoS profile to any of the Policy Profiles at the bottom of the QoS window:
Navigate to Configuration > Security > Local Policy and create a new Service Template:
Specify Ingress and Egress QoS profile that was created in the previous step. An access list can also be applied in this step. If no VLAN change is necessary, leave the vlan field empty:

Navigate to Policy Map tab and click add:
Set Policy Map name and add new criteria. Specify the Service Template that was created in the previous step and select the Device Type this template should be applied to. In this case, Microsoft-Workstation is used. If multiple policies are defined, the first match is used.

One other common use case would be to specify OUI based match criteria. If a deployment has a large number of scanners or printers of the same model, they usually have the same MAC OUI. This can be used to apply specific QoS DSCP marking or an ACL:

In order for WLC to be able to recognize the youtube and facebook traffic, Application visibility needs to be turned on. Navigate to Configuration > Services > Application Visibility enable visibility for the Policy Profile of your WLAN:
Finally, make sure that under the policy Profile the HTTP TLV Caching, DHCP TLV Caching, Global device Classification are enabled and that Local Subscriber Policy is pointing to the Local Policy map that was created in one of the previous steps:

After the client connects, it is possible to check if the local policy has been applied and test if youtube and facebook are actually blocked. Output of the show wireless client mac-address [MAC_ADDR] detailed will contain:
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

Radius Profiling for Advanced Policy Sets in Cisco ISE

With RADIUS profiling enabled, the WLC forwards profiling information to the ISE. Based on this info, it is possible to create advanced authentication and authorization rules. This article does not cover ISE configuration. Please refer to the Cisco ISE Profiling Design Guide for more information. This workflow usually requires the use of CoA, so make sure it is enabled on the 9800 WLC.

Profiling in FlexConnect Deployments

Central Authentication, Local Switching

In this setup, both Local and RADIUS profiling will continue to work exactly like described in previous chapters. If AP goes into standalone mode (AP loses connection to the WLC), device profiling will stop working and no new clients will be able to connect.

Local Authentication, Local Switching

If AP is in connected mode (AP joined to the WLC), profiling will continue to work (AP will send a copy of client's DHCP packets to the WLC to perform the profiling process). Despite profiling working, since authentication is performed locally on the AP, profiling information cannot be utilized for any Local Policy configuration or RADIUS profiling rules.

Troubleshooting

Radioactive Traces

The easiest way to troubleshoot client profiling on the WLC is via radioactive traces. Navigate to Troubleshooting > Radioactive Trace, enter the client’s wireless adapter MAC address and click Start:
Connect the client to the network and wait until it reaches run state. Stop the traces and click **Generate**. Make sure that Internal Logs are enabled (this option only exists in 17.1.1 releases and above):

Relevant snippets from the radioactive trace can be found below:

Client getting profiled by WLC as Microsoft-Workstation:
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

WLC caching the device classification:

WLC finding the device classification inside the cache:

WLC applying local policy based on classification:

WLC sending accounting packets containing DHCP and HTTP profiling attribute:

Packet Captures

In a centrally switched deployment, packet captures can be performed on the WLC itself. Navigate to Troubleshooting > Packet Capture and create a new capture point on one of the interfaces that are in use by this client. It is required to have SVI on the vlan in order to perform capture on it, otherwise take the capture on the physical port itself.