aruba
a Hewlett Packard Enterprise company

TECHNICAL WHITEPAPER

DEVICE FINGERPRINTING

ARUBAOS-SWITCH VERSION 16.06

PURPOSE

Device fingerprinting helps categorize the devices by analyzing the data sent by the end devices. When a specific device is fingerprinted, the details can be used to provide controlled network access and bandwidth for the end devices by ClearPass. Administrators can create appropriate access and enforcement policies in ClearPass during authentication. For example, the devices which are fingerprinted or profiled as computers will be given access to specific VLAN and the devices which are categorized as phones will be given access to another VLAN. Device fingerprinting can be enabled per-port.

Fingerprinting of end devices is achieved by configuring switch to analyze the traffic patterns and send only the required piece of information to ClearPass for parsing. Switch collects the protocol data sent by the end clients and forward the same data securely to ClearPass. This data is then used by ClearPass to fingerprint the end devices that can be further used to set network access policies.

Device fingerprinting is a feature that monitors various protocol traffic from end devices and extracts specific information from the packets based on user configuration. The information collected from the end devices will be sent to ClearPass for further analysis and profiling. In the current release devices that supports device fingerprinting feature monitors HTTP, DHCP, LLDP and CDP traffic from end points and extracts data from these protocols based on user configuration.
The information collected from these devices may include all or some of the following:

- Type of the device
- Type of the vendor
- Operating system of the device
- Version of the operating system

CONFIGURATION

The prerequisites for implementing this feature in ArubaOS-Switch is as follow. Configure the following commands before implementing Device Fingerprinting in ArubaOS-Switch.

```
radius-server host <cppm ip address>
radius-server cppm identity <username> key<password>
```

The username and password is a ClearPass local admin account with the API Administrator privilege.

Another aspect of implementing Device Fingerprinting is ClearPass server certificate installation. The signing CA of the ClearPass HTTP server certificate must be copied to the switch for successful Device Fingerprinting operation. This is the same configuration as Downloadable User Roles (DUR).

The following commands are used to copy CA certificate on ClearPass to the switch:

1. To create TA certificate.
   `crypto pki ta-profile <TA profile name>`
2. To copy CA certificate to the TA profile.
   `copy tftp ta-certificate <TA Profile name> <TFTP Ip Address> <TA Certificate Name>`

The following topology shows the typical implementation of Device Fingerprinting. Device Fingerprinting is recommended to

be implemented in the Access Switches.

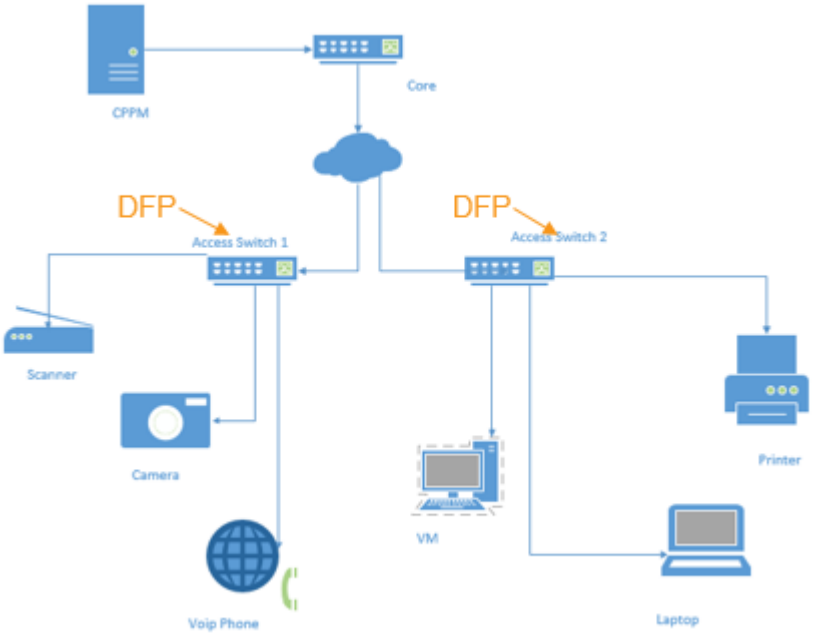

Figure 1. Sample Device Fingerprinting topology

Device Fingerprinting workflow is described next.

1. User creates DFP Profile (Profile contains network protocols and options that need to be extracted. Default options will be provided for every network protocol that is supported in Device Fingerprinting).
2. Users can apply profile created to one or all the ports.
3. Upon applying the profile to a port, switch will intercept the packets.
4. Once the packet from end point device hits the programmed hardware rules, packets are sent to master CPU for processing.
5. Processing involves parsing the packet and extracting the fields from the packet based on the profile configuration.
6. Details that are parsed from packets are stored in a data structure called as client database.
7. Client details are sent to ClearPass based on a timer. ClearPass uses this data to fingerprint the device. Default timer expiry is 2 minutes.

The switch configuration is explained next.

1. Connect end clients to the DUT.
2. Create DFP Policy

```
device-fingerprinting policy "hello"
        dhcp
        http
        lldp
        cdp
```

3. Apply policy on a port

```
device-fingerprinting apply policy hello 2/A5
```

4. Check for client-status

```
show device-fingerprinting client-status
```

    a. Initially it will show “Data not collected”

```
Port  Client MAC      Finger Printing Status
----- --------------- ----------------------
2/A5  7446a054d1a2    Data not collected
```

b. When client sends packets to the collector(Switch), it will be "Data collected"

```
Port  Client MAC      Finger Printing Status
----- --------------- ----------------------
2/A5  7446a054d1a2    Data collected
```

c. When the data is extracted from database and sent to ClearPass successfully, it will be "Completed"

```
Port  Client MAC      Finger Printing Status
----- --------------- ----------------------
2/A5  7446a054d1a2    Completed
```

Note:

There is yet another state which is In Progress – The client fingerprint data is either post into ClearPass or client details are being pulled. If we have only one protocol configured in the profile then, that profile is applied to the port. For example, when the end client is fingerprinted through DHCP, it will be removed from client-status and present in client-details. That is to say, you will not be able to see data completed if all the protocols configured have been received by the device, and that client has been fingerprinted through all of them.

5. Check for client-details and verify

```
show device-fingerprinting client-details
MAC Address         Device Name         Device Category           Device Family
-------------       ------------        ----------------          --------------
7446a054d1a2        HP IP Phone         VoIP Phone                HP
```

The following list contains other set of related CLI commands for Device Fingerprinting.

device-fingerprinting timer - Configures the timer for switch to send the client data to CPPM. The default time is 120 seconds. The time range is 60 to 300 seconds.

```
device-fingerprinting timer <60-300>
```

device-fingerprinting client-limit - Sets the maximum client limit that can be fingerprinted on a port. The default client limit is two. The client limit range is 2 to 8.

```
device-fingerprinting <port num> client-limit <2-8>
```

device-fingerprinting <port num> incoming-clients-only - Enables the fingerprinting for the new clients. To execute this command, device fingerprinting feature must be enabled on the ports.

```
device-fingerprinting <port num> incoming-clients-only
```

The following screenshots shows the Device Fingerprinting configuration done on ClearPass.

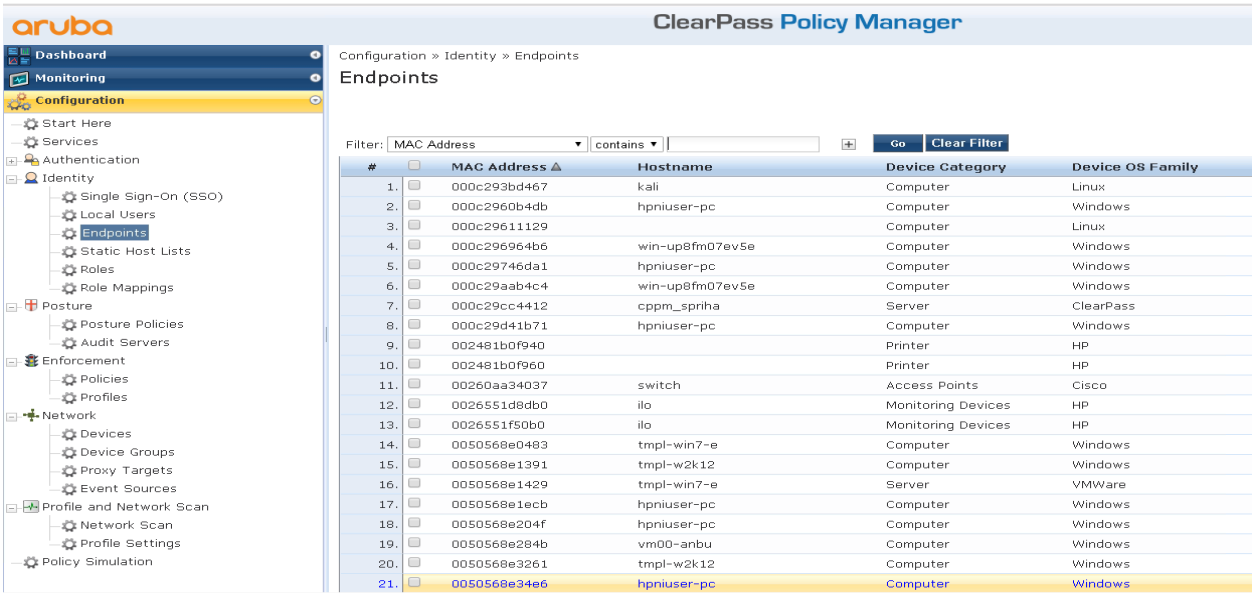

Figure 2. Device Fingerprinting configuration for ClearPass for an endpoint

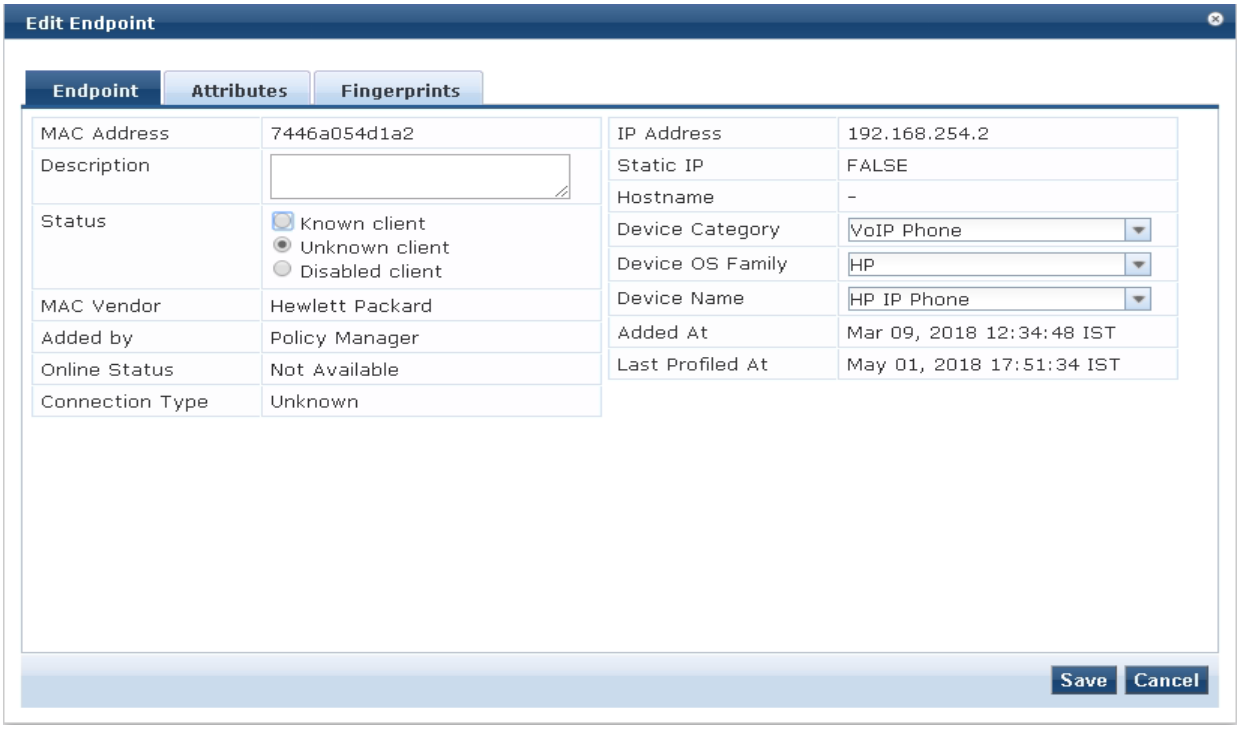

Figure 3. Endpoint details in ClearPass

The following are the current limitation of Device Fingerprinting in ArubaOS-Switch Version 16.06.

- Device fingerprinting cannot be enabled on the same port as Port-Based Tunneling (PBT). When the controller is not reachable, then the tunnel node server fallback local switching is configured for device fingerprinting to work.
- If the client does not send the configured protocol or configured options for some protocols, the fingerprinting cannot be completed.

- HTTP fingerprinting works only when the traffic is received on Port 80.
- Client entries are automatically removed from the client status table after 30 minutes.
- Device fingerprinting and Dynamic Segmentation cannot work together on the same port when the switch is enabled (globally, irrespective of VLAN configuration) with DHCP snooping.
- If the fingerprinting policy is already applied on the ports and the client limit is changed, then the effect only applies for the runtime clients or after interface flap.

The following some troubleshooting steps to perform in the event Device Fingerprinting is not working.

- Device Fingerprinting client details is blank.
    - Make sure that the ClearPass is reachable via TCP 443
    - Make sure that the valid username and password are used.
    - Verify the client's MAC-Address present in '`show mac-address`' for ports where device fingerprinting is enabled.
    - Run the client status output and see the client fingerprint state. If the clients are not in completed state, then the fingerprinting has not been successfully completed.
    - Make sure that the profile is applied on the ports.
    - Make sure that the port status is up.
    - Verify that the client mac-address present in show mac-address for ports where device fingerprinting is enabled.
    - Make sure that the profile is applied on the ports.
    - Try port flap.
    - If status is "Data not collected" - Connect Wireshark and check whether client is sending configured protocol.
        - Configured protocols include DHCP, HTTP, LLDP, CDP.
        - There are options/TLV that can be configured for DHCP, LLDP and CDP. By default, some options are present. If the client does not send these options, the status for that client will be in "Data not collected".
    - If status stays in "Data collected" - Verify the reachability to ClearPass.

SUPPORTED PLATFORMS

Device Fingerprinting feature is supported on the following ArubaOS-Switch running software version 16.06. This feature is also supported in both VSF and Stack configuration for the following switches.

- Aruba 2930F/M Series Switch
- Aruba 3810M Series Switch
- Aruba 5400R Series Switch (Both V2 and V3 mode)