# DHCP FINGERPRINTING WITH Aruba Instant

How do I configure DHCP Fingerprinting on Aruba Instant?

## Introduction

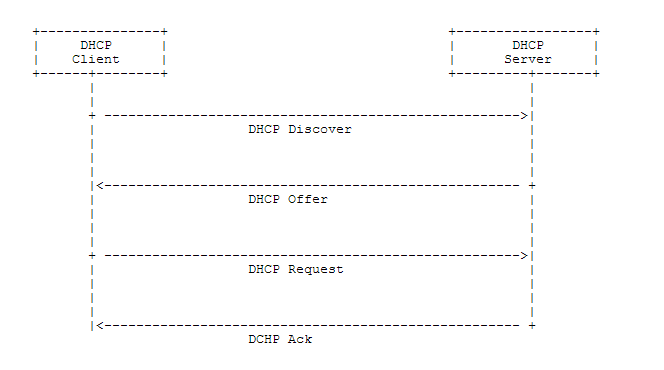
With organizations encouraging corporate users to bring their own device to work; IT staff faces the challenge of differentiating between the devices. Aruba Instant’s Mobile Device Access Control can differentiate devices based on:

1. DHCP Fingerprinting
2. EAP Type

This guide provides background information on DHCP fingerprinting and walks through the configuration, troubleshooting steps.

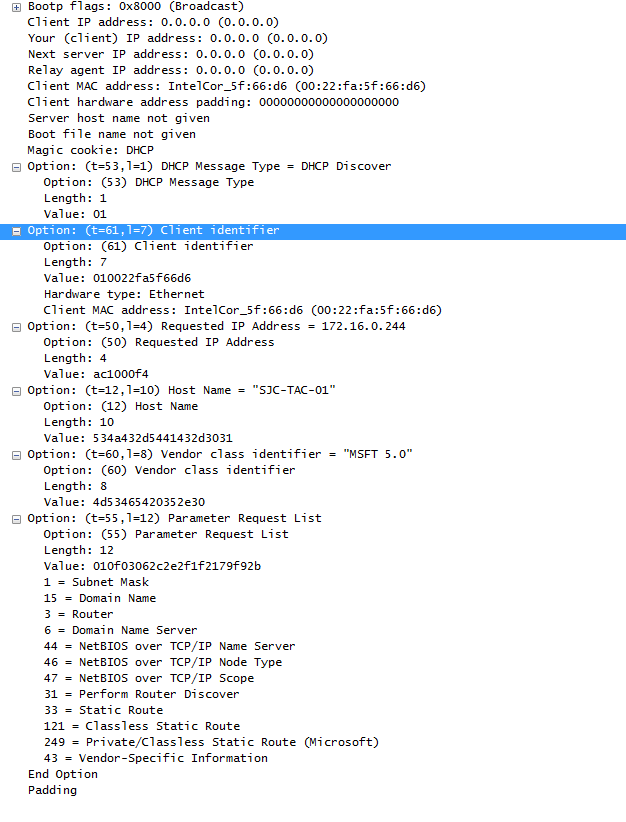
## What is DHCP Fingerprinting?

DHCP is a 4-step client – server exchange through which the client obtains an I.P. address and other network parameters such as gateway I.P. address, DNS server from the Server. Below diagram is an overview of client-server transaction.



Along with the actual request; the DHCP messages carry “DHCP Options” – a set of configuration parameters and other control information. These options can be used to uniquely identify a device type / OS type.

Below is an example of DHCP Options from a Windows 7 client’s DHCP Discover.



As it can be seen in above example; all the DHCP Options are of the format:: [**Option][Length][Value]** where option is the Hex value of the Option number. Example :: Option 61 would be 3D in Hex.

Aruba Instant’s DHCP fingerprinting uses only the Option & Value. Example:: DHCP Fingerprint for Option 61 would be 3D010022FA5F66D6 (See above screenshot).

The DHCP Fingerprinting is based on inspecting the DHCP options of DHCP Discover & Request i.e. client initiated DHCP traffic.

## Which Options are Useful?

Below is the list of DHCP options which can be used for role derivation. It should be noted that::

* Not all devices send all options. Example :: Apple Devices don’t send Option 60
* Option 12 is configurable by end-user i.e. less reliable.

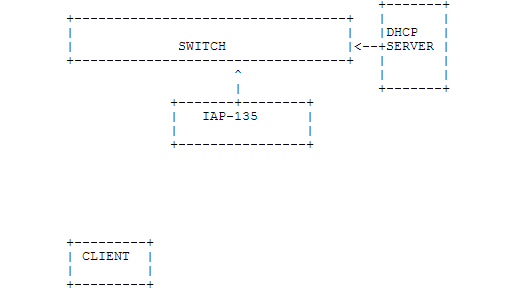
|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Explanation** | **Decimal  Value** | **Hex  Value** |
| Hostname | The name of the client device. | 12 | 0C |
| Parameter Request List | The configuration values requested by the client | 55 | 37 |
| Vendor Class Identifier | Vendors use the option to convey configuration information about the client to the Server. | 60 | 3C |
| Client Identifier | Clients use this option to uniquely identify themselves and value corresponds to the MAC address of client. | 61 | 3D |
| Client FQDN | The FQDN name of the client with the domain name. | 81 | 51 |

## Test Environment

The following software and hardware are used in this document to illustrate the concept and configuration steps.

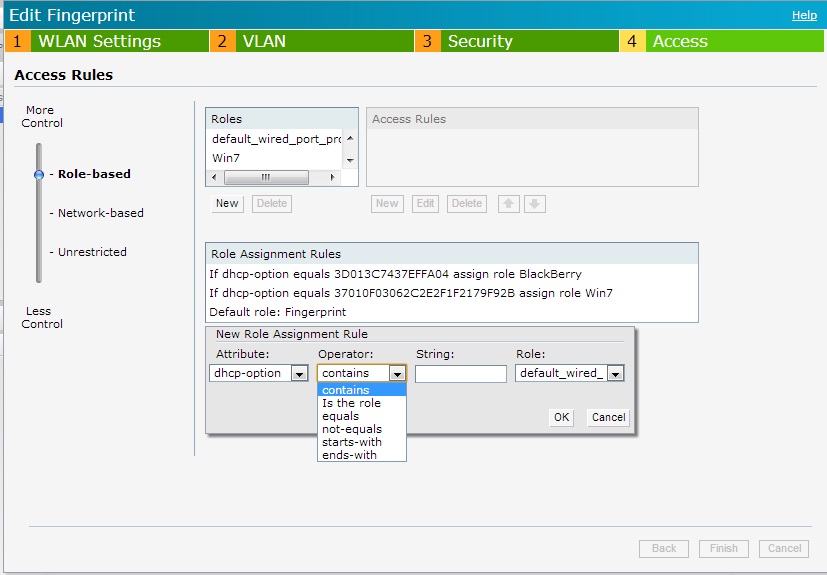
|  |  |
| --- | --- |
| Hardware | Aruba Instant AP 135 |
| Software | Aruba Instant 6.2.0.0-3.2.0.3 |

## Network Topology



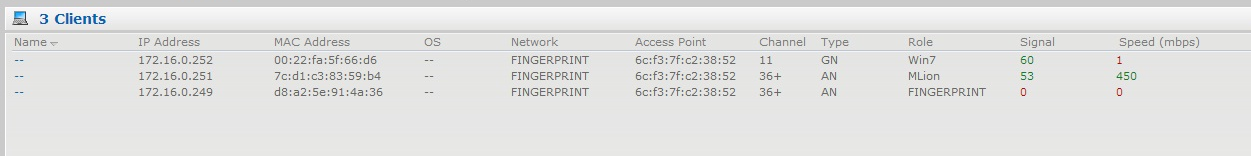
## Configuration

Role assignment via DHCP-Option is available under Access tab of SSID configuration. Below is an example screenshot. If a client doesn’t match any of the rules; it would be assigned the Default role (In this example; Fingerprint)



## Validation

The role assignment can be validated by checking the Clients tab of the User Interface. In the below example; the first two clients have matched a rule and been assigned corresponding rule (Win7 & MLion). The third didn’t match any rule and was assigned the default role.



## Feature Notes

* As of 3.1 release; DHCP-Option role derivation isn’t supported with Captive Portal authentication.
* When there are multiple rules which a client would matches; the first rule is used to derive role. Hence; the rules must be ordered from most specific to least specific.
* If a VLAN is mapped to the ROLE deriver via DHCP-Option; it will not take effect.

## Device Fingerprints

Below is a table which includes fingerprints for major operating systems.

|  |  |  |
| --- | --- | --- |
| **Device** | **Option** | **Value** |
| Apple iOS | 55 | 370103060F77FC |
| Android (Galaxy Note running ICS) | 55 | 37012103061C333A3B |
| Blackberry | 55 | 370103060F |
| Blackberry | 60 | 3C426C61636B4265727279 |
| Windows Vista / 7 | 55 | 37010F03062C2E2F1F2179F92B |
| Windows XP (Sp3, Home, Professional) | 55 | 37010F03062C2E2F1F21F92B |
| Windows XP, Vista, 7 | 60 | 3C4D53465420352E30 |
| Windows 7 Phone | 55 | 370103060F2C2E2F |
| OS X upto 10.7 | 55 | 370103060F775FFC2C2E2F |
| OS X 10.8 | 55 | 370103060F775FFC2C2E |

## Sample Scenarios

### Give special privilege to a specific user

There maybe instances where one specific user / set of users (example :: CEO’s cellphone) must be treated differently. Option 61 can be used to achieve this. As Option 61 is based on the MAC address; the device can be uniquely identified and placed in a specific role. It must be noted that Option 61 based rule must always be on top of the rule list to ensure it gets hit first.

### Windows Devices

#### Rule for Windows XP, Vista and 7

All three OS versions send MSFT 5.0 for Option 60.

DHCP-Option value equal to 3C4D53465420352E30 can be used to classify all three latest Windows Client OS versions (i.e. XP, Vista & 7).

#### Rule for Windows Vista and 7 alone

DHCP-Option value equal to **37010f03062c2e2f1f2179f92b** can be used to classify Windows Vista & 7 OS devices.

#### All Windows Devices from Windows 95

A starts-with “**37010f03062c2e2f**" rule can be used to classify all Windows Client OS devices from Windows 95 till Windows 7.

### Apple Devices

#### iOS Devices

DHCP-Option value equal to **370103060f77fc** can be used to classify iOS devices

#### All Apple Devices

A rule with DHCP-Option value starts with **370103060f77** can be used to classify all iOS and Mac OS X devices.

## Troubleshooting

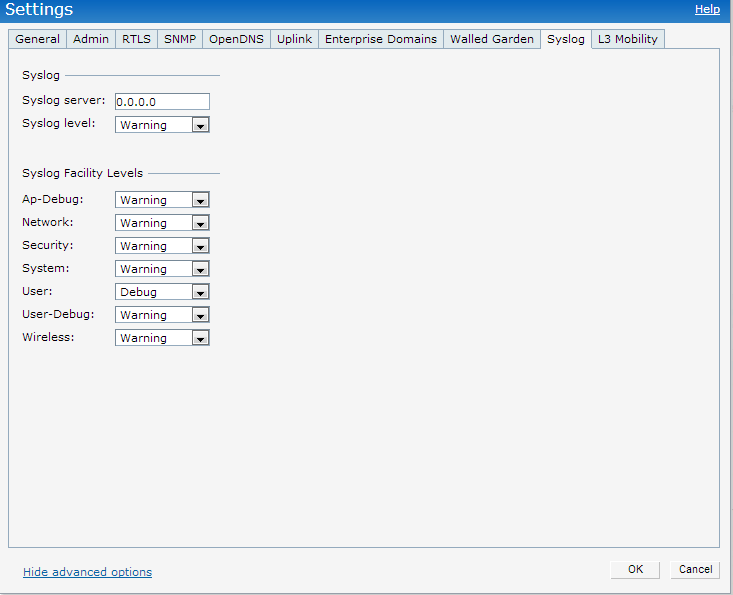
There can be two cases a) Clients hitting the wrong rule b) Client not hitting the rule.

For the case client hitting the wrong rule; ensure the rules ordered from most specific rule to least specific. This would ensure the client hits the right rule i.e. first match.

For the case of client not hitting the rule; we would need to validate if the DHC-Option value used in configuration is right.

With logging level set to debug for User category; Instant would be able to the DHCP fingerprint and role derivation information.

To enable debugging; navigate to Settings --> Show Advanced Options --> Syslog --> User --> Debug.



With debugging enabled; the required information is available under “AP Log User” option under Support tab. Optionally; the output can be filtered using “DHCP”. Below example shows role derivation for a client which matched “Win7” rule.

