



ArubaOS DHCP Fingerprinting

Version 1.0

Copyright

© 2011 Aruba Networks, Inc. AirWave®, Aruba Networks®, Aruba Mobility Management System®, Bluescanner, For Wireless That Works®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFprotect®, The All Wireless Workplace Is Now Open For Business, Green Island, and The Mobile Edge Company® are trademarks of Aruba Networks, Inc. All rights reserved. Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice. While Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, Aruba will assume no responsibility for any errors or omissions.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (“GPL”), GNU Lesser General Public License (“LGPL”), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Warning and Disclaimer

This guide is designed to provide information about wireless networking, which includes Aruba Network products. Though Aruba uses commercially reasonable efforts to ensure the accuracy of the specifications contained in this document, this guide and the information in it is provided on an “as is” basis. Aruba assumes no liability or responsibility for any errors or omissions.

ARUBA DISCLAIMS ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESSED, IMPLIED, OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, ACCURACY, AND QUIET ENJOYMENT. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF ARUBA EXCEED THE AMOUNTS ACTUALLY PAID TO ARUBA UNDER ANY APPLICABLE WRITTEN AGREEMENT OR FOR ARUBA PRODUCTS OR SERVICES PURCHASED DIRECTLY FROM ARUBA, WHICHEVER IS LESS.

Aruba Networks reserves the right to change, modify, transfer, or otherwise revise this publication and the product specifications without notice.



www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

Chapter 1:	Introduction	4
	Reference Material	5
Chapter 2:	Deploying DHCP Fingerprinting	6
	Prerequisites	6
	Product Availability	7
	What is a DHCP Fingerprint?	7
	Identifying a DHCP Fingerprint	9
	User Role Creation	11
	User Role Derivation	15
Chapter 3:	User Role Life Cycle	17
	Connecting to the Wireless Network	17
	802.1X Authentication	18
	DHCP Exchange	19
	Validating DHCP-Derived User Roles	19
	Conclusion	20
Appendix A:	Validated DHCP Fingerprint	21
Appendix B:	Contacting Aruba Networks	22
	Contacting Aruba Networks	22

Chapter 1: Introduction

The explosive growth of mobile devices has challenged the network IT staff because mobile devices lack the option to connect using Ethernet, which is the dominant wired access technology. Leading industry analyst forecasts predict that by 2015 only 15% of the devices will have built-in Ethernet capability, as shown in Growth of mobile devices . As more of these devices connect using the enterprise wireless LAN, network administrators have noted that an employee typically has gone from using a single device to using three or more devices.

As network engineers get ready to support large numbers of smartphones and tablets in addition to laptops and desktops, they are realizing the importance of reliably identifying mobile devices. Gaining visibility into mobile device types is essential for network engineers to build granular access policies to maintain security and quality of service (QoS) for critical enterprise applications. This application note describes one such tool, ArubaOS DHCP Fingerprinting, which empowers the network engineers to reliably identify devices and to build and enforce device-specific policies.

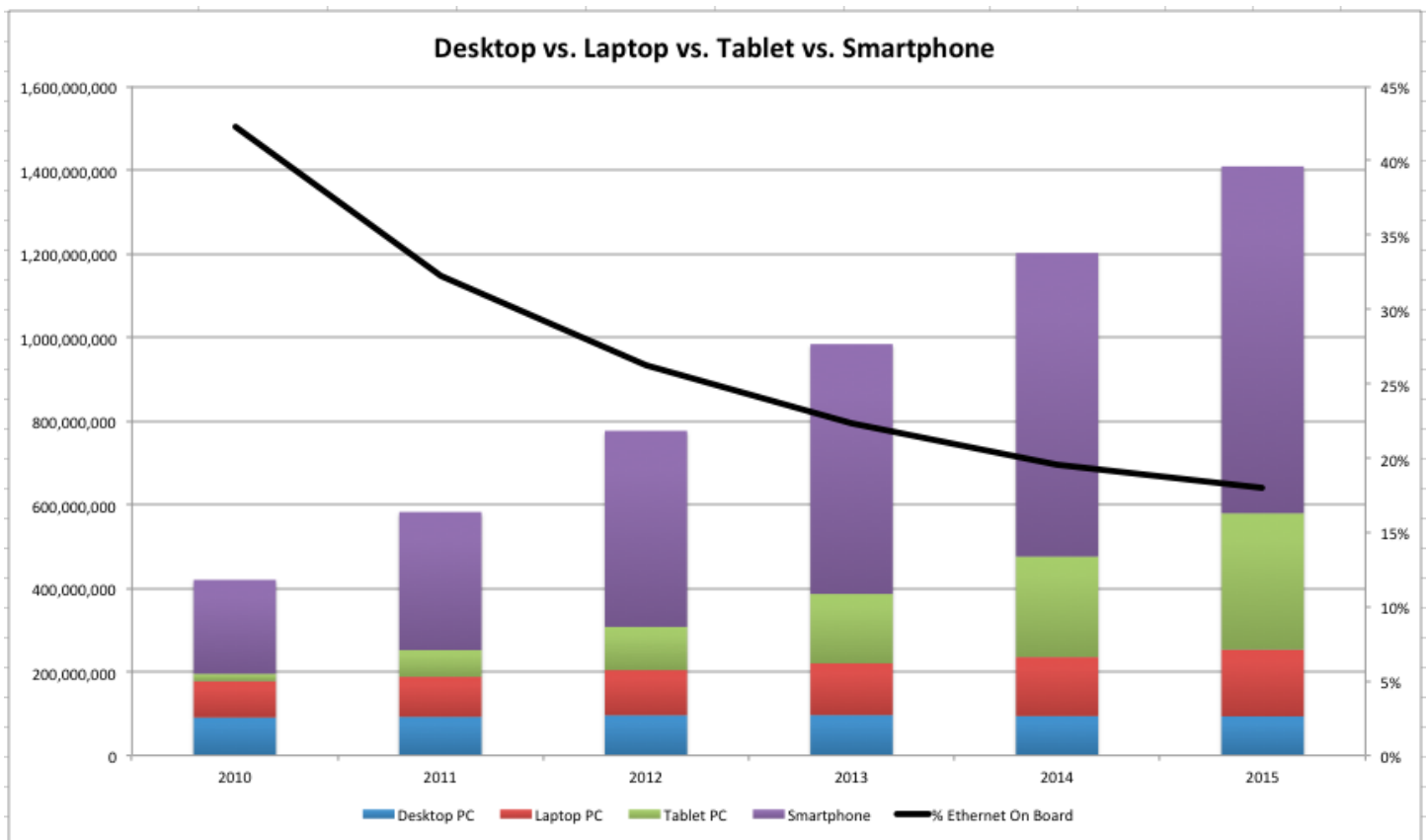


Figure 1 Growth of mobile devices

Table 1 lists the current software versions for this guide.

Table 1 Aruba Software Versions

Product	Version
ArubaOS™ (mobility controllers)	6.1
ArubaOS (mobility access switch)	7.0
Aruba Instant™	1.1
MeshOS	4.2
AirWave®	7.3
AmigopodOS	3.3

Reference Material

- This guide assumes a working knowledge of Aruba products. This guide is based on the network detailed in the *Aruba Campus Wireless Networks VRD* and the *Base Designs Lab Setup for Validated Reference Design*. These guides are available for free at <http://www.arubanetworks.com/vrd>.
- The complete suite of Aruba technical documentation is available for download from the Aruba support site. These documents present complete, detailed feature and functionality explanations outside the scope of the VRD series. The Aruba support site is located at: <https://support.arubanetworks.com/>. This site requires a user login and is for current Aruba customers with support contracts.

Chapter 2: Deploying DHCP Fingerprinting

DHCP fingerprinting is used in conjunction with user roles on the Aruba Mobility Controller. When a user authenticates, their device type is taken into account. Based on that device type, a new role can be assigned to the device, such as restricting access to certain protocols or completely blocking access. Because the system relies on user-defined roles, each organization can develop a system that meets their unique requirements.

Prerequisites

This section describes the prerequisites and dependencies for the ArubaOS DHCP fingerprinting feature.

1. The ArubaOS DHCP fingerprinting feature is available on the mobility controller and mobility access switch platforms running ArubaOS version 6.0.1 or later.
2. The PEFNG license must be present on the platform to assign user roles using the ArubaOS DHCP fingerprinting feature.
3. Clients must be set up to request IP addresses automatically using DHCP.
4. The controller must be in the data path of DHCP exchange, but it does not have to be the DHCP server.
5. There are additional requirements based on the forwarding mode of the AP. [Table 2](#) lists the forwarding mode and platform dependencies.

Table 2 DHCP Fingerprinting Availability by Forwarding Mode and Platform

Platform	Forwarding Mode	DHCP Fingerprinting Available
Campus and remote AP	Tunnel mode	Yes
Campus and remote AP	Bridge mode	No
Campus and remote AP	Decrypt-tunnel mode	Yes
Remote AP	Split-tunnel mode	Yes. Limited to VLANs that are tunneled to the controller.
Mobility access switch	Tunneled node	Yes

Product Availability

Table 3 describes the DHCP fingerprint availability by platform.

Table 3 Product Availability

Platforms	DHCP Fingerprinting Available
Mobility Controller – 600, 3000, and M3 Series platforms	Yes
All Mobility Access Switch platforms	Yes. Limited to VLANs that are tunneled to the controller
All Instant AP platforms	No

What is a DHCP Fingerprint?

DHCP is a client/server protocol. As shown in Figure 2, the DHCP client exchanges a series of packets with the DHCP server to obtain a unique IP address and other important networking information, such as the default gateway and DNS server.

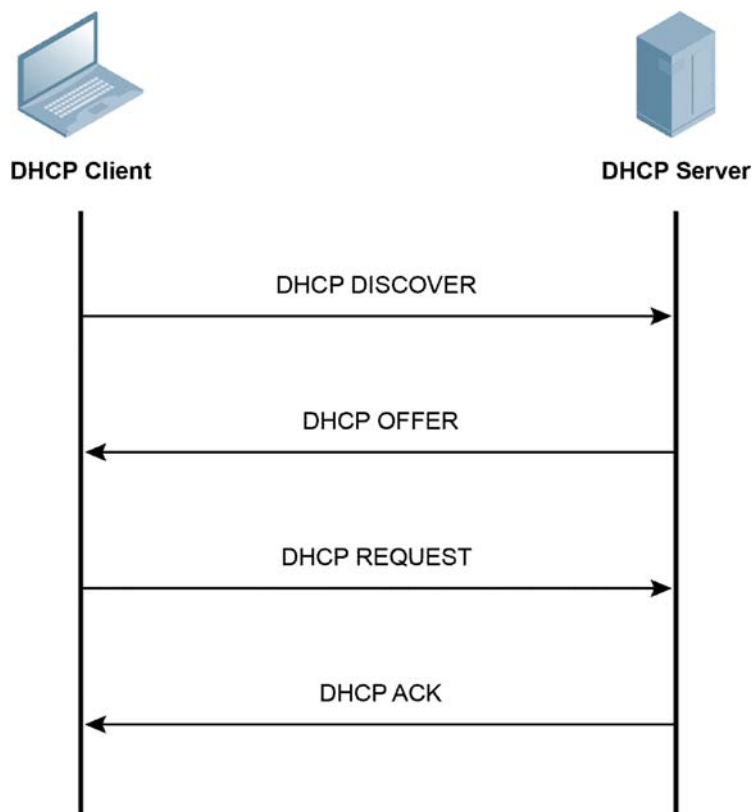


Figure 2 DHCP protocol exchange

However, the DHCP protocol is not limited to obtaining basic IP networking information. It includes the flexibility to exchange vendor-specific information about the hardware or operating system of the device. This exchange is done by using DHCP options as defined by RFC 2132 (<http://www.ietf.org/rfc/rfc2132.txt>). Use of DHCP options is vendor-, device-, and OS-dependent, which creates significant differences in the DHCP packets generated by various devices and thus constitutes a DHCP

The ArubaOS DHCP fingerprinting feature instructs the stateful firewall to inspect the DHCP packet exchange and identify the device or OS type. Firewall rules can then be used to derive roles for the specific device or OS type.

Identifying a DHCP Fingerprint

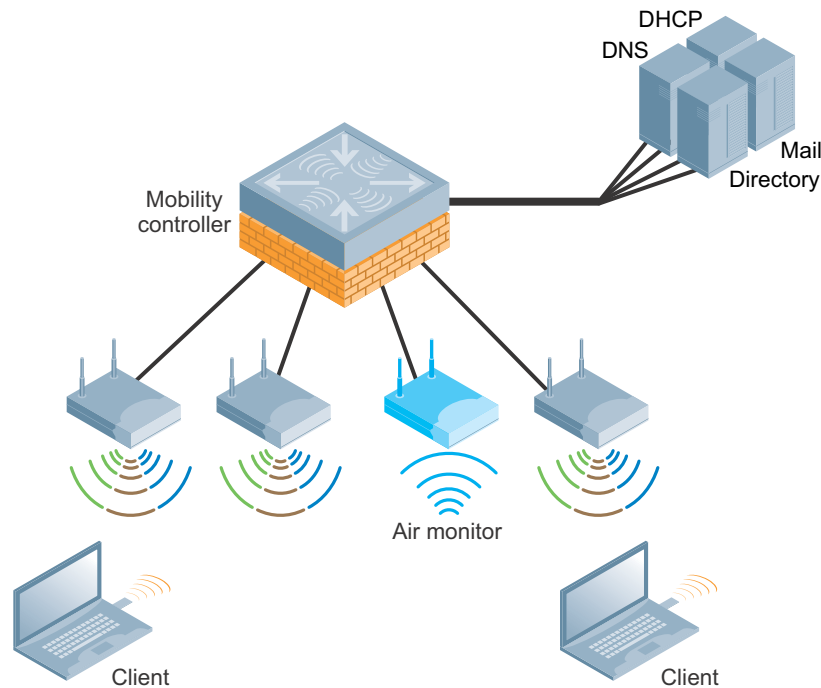


Figure 4 Network diagram with an ArubaOS controller in the DHCP data path

ArubaOS DHCP fingerprinting relies on the stateful inspection of DHCP packet exchange, so it is required that the Aruba Mobility Controller is in the data path of the DHCP exchange. However, the mobility controller is not required to be the DHCP server. ArubaOS stateful firewall logs the DHCP options in the DHCP packets along with the MAC address of the client.

To begin the process of examining a DHCP fingerprint, some debugging commands need to be set to make the packets visible. This process can be done either from the web interface or the CLI. We are looking for a value that is unique to a class of device. In cases where more than one DHCP fingerprint is found, any can be used. Typical values of DHCP options are hex: 0c, 37, 3c, or 51. These values correspond to DHCP option numbers: 12, 55, 60, or 81. The goal is to find a value that is unique to that device.

If multiple clients are connecting at the same time, be sure to select the DHCP signature that matches the test device MAC address. Log messages can also be restricted to show output that matches the specific MAC address of the test device. It is a best practice to validate the DHCP signatures using several devices of same type. For a list of validated DHCP signatures developed by the Aruba QA team, see [Appendix A: Validated DHCP Fingerprint on page 21](#).

Using the WebUI

1. Set the logging level for dhcp sub-category to level **debugging**. Navigate to **Configuration → Management → Logging Levels**.
2. Navigate to **Monitoring → Debug → Process Logs**.
3. From the right-side frame, select the **Search** function and select Filter Criteria: **Include** and String: **Options**. Click **Display**. The logs automatically refresh.

Debug > Logs

The screenshot shows the 'Process Selection' interface with the following settings:

- Logs:** All
- Filter Criteria:** Include
- Display Amount:** 100
- String:** options

Buttons: Display, Reset, Save As, Export

Figure 5 Filter options

4. Ensure that the wireless client is set up for DHCP and connect to the wireless network.
5. Watch the filtered logs section for matching log messages. When the client sends out the DHCP DISCOVER or REQUEST packet, a log message that contains the DHCP option is generated. [Figure 6](#) shows a log message from an Apple iPad device with MAC address a4:d1:d2:1b:40:31.

Time	Log
Sep 7 11:38:08	dhcpcdwrap[1829]: <202536> <DEBUG> dhcpcdwrap dhcp Datapath vlan900: REQUEST a4:d1:d2:1b:40:31 reqIP=192.168.200.248 Options 37:0103060f77fc)39:05dc 3d:01a4d1d21b4031 36:c0a8c814 0c:6970616432

Figure 6 Using WebUI log filtering to identify a DHCP fingerprint

The numerals displayed in the log message correspond to DHCP option 55 (37 in hex notation). In hexadecimal notation, option code 37 is followed by its operand values. The combined string forms the DHCP fingerprint **370103060F77FC**.

Using the CLI

1. Ensure that the wireless client is set up for DHCP and connect to the wireless network. Note the wireless client MAC address. From the CLI, enter the “config terminal” context and enable logging level debug for DHCP.

```
(config)# logging level debugging network
```

2. Issue the CLI command to show log entries that match the MAC address of the client device being fingerprinted.

```
(config)#show log network all | include Options
```

3. Watch the filtered log messages for DHCP options. The output in [Figure 7](#) is for an Apple iPad device with MAC address a4:d1:d2:1b:40:31.

```
(LC1-Sunnyvale-6000) (config) #show log all | include Options
Sep 7 11:38:08 dhcpdwrap[1829]: <202536> <DEBUG> |dhcpdwrap| |dhcp| Datapath vlan900: REQUEST
a4:d1:d2:1b:40:31 reqIP=192.168.200.248 Options 37:0103060f77fc 39:05dc 3d:01a4d1d21b4031
36:c0a8c814 0c:6970616432
```

Figure 7 Using CLI log filtering to identify a DHCP fingerprint

From the log message output, we find DHCP options 55, 12, 50, and 51 (hex 37, 0C, 32, and 33 respectively). Based on Aruba internal testing, we have found that reliable DHCP signatures include DHCP options 12, 55, 60, and 81. We can use any of these options to build a DHCP signature. For example, if we select the option 55 (hex 37), to create a DHCP fingerprint, drop the colon (":") and include all the hex numerals before and after the colon.

The DHCP fingerprint for device with MAC a4:d1:d2:1b:40:31 is **370103060F77FC**.

User Role Creation

In an Aruba user-centric network, every device is associated with a user role based on login credentials, among other things. This same concept is extended to derive roles based on device type. For detailed configuration steps for roles and policies, refer to *ArubaOS 6.1 User Guide*, Chapter 12.

In our example, an enterprise has a mobile device access policy for two popular mobile device platforms, Apple iOS and Android, as shown in [Table 4](#). Each class of device has a desired policy as determined by the organization. These policies are implemented by defining rules and applying them to the appropriate device-specific user role.

Table 4 Sample Mobile Device Access Policy for Android and iOS Devices

Mobile Device Platform	Enterprise Access Policy
Apple iOS	Allow access to the corporate internal network via https only. Allow full access to the Internet.
Android	Deny all access to the corporate internal network. Allow full access to the Internet.

When devices connect to the WLAN network, they require a minimum set of services such as access to DHCP and DNS services. These services are defined in the Common-Policy and they are common to Apple iOS and Android device roles. Android devices are blocked from accessing the corporate internal network, while Apple iOS devices are allowed access to the internal network only through https. This permission is implemented in the block-internal-access and allow-corporate-https policies respectively. Finally, full access to the Internet is achieved by adding the allow-all policy as the last policy in the role.

Configuration for Common Policies Shared by Android and iOS Devices

```
ip access-list session common
  user any udp 68 deny
  any any svc-dhcp permit
  any any svc-icmp permit
  user alias dns-servers svc-dns permit
```

Security > User Roles > Edit Role(iOS-Device-Role) > Edit Session (common)

User Roles	System Roles	Policies	Time Ranges	Guest Access			
Rules							
IP Version	Source	Destination	Service	Action	Log	Mirror	Queue
IPv4	user	any	udp 68	deny			Low
IPv4	any	any	svc-dhcp	permit			Low
IPv4	any	any	svc-icmp	permit			Low
IPv4	user	dns-servers	svc-dns	permit			Low
<input type="button" value="Add"/>							

Figure 8 Common policies shared by Android devices

Next we will configure the access to internal resources, which will be used for the allow policy for iOS and for the deny policy for Android. For this setup, we will create a network destination alias. Netdestinations allow you to specify blocks of addresses and later make changes to those blocks without rewriting firewall policy.

Internal Corporate Network Destinations

```
netdestination Internal-Network
network 10.0.0.0 255.0.0.0
network 172.16.0.0 255.255.0.0
network 192.168.0.0 255.255.0.0
```

Advanced Services > Stateful Firewall > Destinations > Edit Destination (Internal-Network)

Global Setting	White List BW Contracts	Network Services	Destination	BW Contracts
IP Version				
Destination Name				
Invert				
Type	IP Address	NetMask		
network	10.0.0.0	255.0.0.0		
network	172.16.0.0	255.255.0.0		
network	192.168.0.0	255.255.0.0		
<input type="button" value="Add"/>				

Figure 9 Internal corporate network destinations

Next we will create two policies, one that allows corporate resources to be accessed via HTTPS, and one that denies all access to those same resources. First we will configure the iOS policy, then the Android policy.

Configuration for the iOS allow-corporate-https Policy

```
ip access-list session allow-corporate-https
user alias Internal-Network svc-https permit
user alias Internal-Network any deny
```

Security > User Roles > Edit Role(iOS-Device-Role) > Edit Session (allow-corporate-https)

User Roles	System Roles	Policies	Time Ranges	Guest Access				
Rules								
IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range
IPv4	user	Internal-Network	svc-https	permit			Low	
IPv4	user	Internal-Network	any	deny			Low	
<input type="button" value="Add"/>								

Figure 10 Configuration for the iOS allow-corporate-https policy

Configuration for iOS Device Role

```

user-role iOS-Device-Role
  access-list session common
  access-list session allow-corporate-https
  access-list session allowall

```

Security > User Roles > Edit Role(iOS-Device-Role)

User Roles | System Roles | Policies | Time Ranges | Guest Access

Firewall Policies

Name	Rule Count
common	4
allow-corporate-https	2
allowall	1

Add

Figure 11 Policies for iOS device role

Policies for Android Devices

```

user-role Android-Device-Role
  access-list session common
  access-list session block-internal-access
  access-list session allowall

```

Security > User Roles > Edit Role(Android-Device-Role)

User Roles | System Roles | Policies | Time Ranges | Guest Access

Firewall Policies

Name	Rule Count
common	4
block-internal-access	1
allowall	1

Add

Figure 12 Policies for Android devices

User Role Derivation

After a DHCP fingerprint has been identified and the device-specific roles have been created, we can now configure the policy for the devices. To get the correct policy assigned, we use “user rules” to change the devices role. Roles that are derived using DHCP fingerprinting take precedence over those derived using other methods, such as server-derived roles or roles derived using an Aruba vendor-specific attribute (VSA). This precedence means that roles derived by the DHCP fingerprint feature prevail even if the RADIUS server is set up to return a role attribute that is different. This functionality allows users to log into a device such as a laptop and receive a normal role via RADIUS, and then use the same credentials on an iPad and receive a different device role.

Roles are derived based on information learned from DHCP exchange, so devices receive this role after successful 802.11 association and Layer 2 authentication. For this reason, a role derived using DHCP fingerprinting is referred as the post-authentication role. It is important to note that while several ways are available for deriving a role in ArubaOS, DHCP fingerprinting is different from all of them. DHCP fingerprinting operates on attributes that become available after a successful authentication, which extends the role-derivation capability in a powerful way.



DHCP fingerprinting is classified as one of the methods under the user-derived role framework. However, it differs from other methods in an important respect. DHCP fingerprinting has higher precedence than all other role-derivation methods.

To derive device-specific roles from the WebUI and the CLI, follow these steps.

Using the WebUI

1. Navigate to **Configuration** → **Security** → **Authentication**.
2. Click **User Rules**. Click **Add** to add a user-derived rule.
3. Choose a name for the user-derived rule. See example *byod-rules*.
4. Click **Add** to add a new rule set. The screen in [Figure 13](#) is displayed.

Add new rules	
Set Type	Role ▾
Rule Type	DHCP-Option ▾
Condition	equals ▾
Value	370103060F77FC
Roles	iOS-Device-Role ▾
Description	iOS devices
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

Figure 13 Adding rules to derive roles using DHCP Option from WebUI

5. For Set Type, choose **Role** to derive roles.
6. For Rule Type, choose **DHCP-Option**.

7. For Condition, choose **equals**. This rule is set up especially to match DHCP option and its operand values in hex, so equals and starts-with are the only allowed conditions.
8. In the Value field, copy and paste the DHCP fingerprint. Ensure that no colon characters or extra whitespace are included and that only the hex numerals are included.
9. For Roles, choose the device-specific role that was created earlier.

Using the CLI

From the CLI, enter the “config terminal” context and issue the following commands:

```
aaa derivation-rules user byod-rules
  set role condition dhcp-option equals "3C64686370636420342E302E3135" set-value Android-Device-
  Role description "Android devices"
  set role condition dhcp-option equals "370103060F77FC" set-value iOS-Device-Role description
  "iOS devices"
```

Chapter 3: User Role Life Cycle

ArubaOS DHCP fingerprinting provides an easy method to distinguish a user connected on corporate-issued laptop vs. another mobile device. When the corporate user connects to the Aruba system using the corporate laptop and the personal device, they receive different user roles. In this section, we follow the clients through various connectivity states, highlight the relevant configuration profiles, and describe how they influence the selection of user roles.

Connecting to the Wireless Network

When users scan the available wireless networks, they see the SSID that is defined in the SSID profile “corp-employee”. This SSID requires 802.1X authentication. This profile is configured in the Wireless LAN → Virtual AP context.

The screenshot shows the configuration page for the 'Corp-Employee' SSID profile. At the top, there is a dropdown menu for 'SSID Profile' set to 'Corp-Employee', and three buttons: 'Show Reference', 'Save As', and 'Reset'. Below this are two tabs: 'Basic' (selected) and 'Advanced'. The 'Basic' tab contains three sections: 'Network', '802.11 Security', and 'Keys'. The 'Network' section has a 'Network Name (SSID)' field with the value 'Corp-Employee'. The '802.11 Security' section has 'Network Authentication' with radio buttons for 'None', '802.1x/WEP', 'WPA', 'WPA-PSK', 'WPA2' (selected), and 'WPA2-PSK', and 'Encryption' with a radio button for 'AES' (selected). The 'Keys' section is currently empty.

Figure 14 SSID profile for the Corp-Employee wireless network

In a typical enterprise, PEAP with MSCHAPv2 is a popular choice for 802.1X authentication. Users must login with their corporate credentials and passwords. This process is routine on the laptops. The process is similar on mobile devices. Users are now authenticated to the network based on their unique user credentials. The authentication process uses the AAA profile defined in the virtual AP profile as seen in [Figure 15](#).

Configuration > AP Group > Edit "AP-LC1-Sunnyvale-6000"

The screenshot shows the configuration page for the virtual AP 'Corp-Employee-LC1-Sunnyvale-6000'. Under the 'Profiles' section, the 'AAA Profile' is set to 'corp-employee'. Other profiles listed include '802.11K Profile' (default), 'SSID Profile' (Corp-Employee), 'EDCA Parameters Station profile', 'EDCA Parameters AP profile', 'High-throughput SSID Profile' (default), and 'WMM Traffic Management Profile' (corp-wmm).

Figure 15 AAA profile for corp-employee virtual AP profile

802.1X Authentication

The mobile device and laptop complete the 802.1X authentication and four-way handshake and derive the unique Pairwise Master Key (PMK) that is used to secure all further data transactions. Based on the AAA profile “corp-employee”, we see that both clients initially get the “logon” role as defined by the initial role setting. However this role is transient and clients soon migrate to new roles based on the user derivation rules, which are linked to the same AAA profile as shown in [Figure 16](#).

AAA Profile > corp-employee Show Reference Save As Reset

Initial role	logon	MAC Authentication Default Role	guest
802.1X Authentication Default Role	employee	L2 Authentication Fail Through	<input type="checkbox"/>
RADIUS Interim Accounting	<input type="checkbox"/>	User derivation rules	byod-rules
Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--
Device Type Classification	<input checked="" type="checkbox"/>	Enforce DHCP	<input checked="" type="checkbox"/>

Figure 16 Initial role and user derivation rules in the AAA corp-employee profile

DHCP Exchange

At this point, the previously constructed user rule “byod-rules” comes into play. Specifically, when the clients are evaluated against this rule set, the Apple iPad matches the second rule and the corporate Windows laptop does not yield a match. As per our rule definition, the Apple iPad progresses to receive the “iOS-Device-Role”, and the corporate Windows laptop receives the “802.1X Authentication Default” role “employee” as defined by the AAA profile “corp-employee” shown in [Figure 16](#) and [Figure 17](#).

Security > Authentication > User Rules

The screenshot shows the configuration for the 'byod-rules' rule set. It contains two rules:

Priority	Attribute	Operation	Operand	Action	Value
1	dhcp-option	equals	3C64686370636420342E302E3135	set role	Android-Device-Role
2	dhcp-option	equals	370103060F77FC	set role	iOS-Device-Role

Figure 17 Rule set to derive device-specific roles

Validating DHCP-Derived User Roles

To view the client statistics, navigate to the controller **Monitoring** → **Clients** as seen in [Figure 18](#). Verify that devices have been correctly detected and assigned appropriate roles. It is also interesting to note the Device Type column. Here Windows corporate laptops are identified by operating system type even though no DHCP fingerprint has been defined for the Windows corporate laptops.

This operating system identification is a result of a separate but related feature mechanism to detect device types. It operates by parsing the user-agent string (also known as the browser ID) in HTTP packets. This parsing is enabled by the Device Type Classification checkbox in the AAA profile. This feature is enabled by default. The user-agent string can be changed easily by misbehaving applications or intentional user action, which makes them less than reliable for user derivation roles.

The screenshot shows the 'Clients' page with the following data:

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID	AP Name	Phy Type	Age	Roaming Status	Forward Mode
employee1	Win 7	58:94:6b:f1:dc:f8	10.169.154.52	employee	802.1x	Corp-Employee	AP-LC1	802.11a-HT	56 mins	Wireless	tunnel
andy	Win Vista	00:1a:73:54:97:a6	10.169.152.51	employee	802.1x	Corp-Employee	AP-LC1	802.11g-HT	3 hrs 31 mins	Wireless	tunnel
employee1	iPad	a4:d1:d2:1b:40:31	10.169.150.51	iOS-Device-Role	802.1x	Corp-Employee	AP-LC1	802.11a-HT	56 mins	Wireless	tunnel

Figure 18 Monitor clients and verify the user roles from the WebUI

Conclusion

Enterprises and employees are rapidly adopting next-generation smartphones and tablet devices. Wireless is the only way to connect these devices to the network and WLAN is the primary method of connecting to an enterprise network. IT staff require tools that enable them to control the network usage, applications, content, and bandwidth and gain greater visibility into the user and type of devices. ArubaOS delivers a powerful new tool, DHCP fingerprinting, which enables IT staff to create and enforce granular policies per device, per application, and per user. This added functionality is made possible using the same Aruba WLAN infrastructure without adding additional appliances or re-architecting the network.

Appendix A: Validated DHCP Fingerprint

These device fingerprints must be used with an exact-match rule in ArubaOS.

Device	DHCP Option	DHCP Fingerprint
Apple iOS	Option 55	370103060F77FC
Android	Option 60	3C64686370636420342E302E3135
Blackberry	Option 60	3C426C61636B4265727279
Windows 7/ Vista Desktop	Option 55	37010f03062c2e2f1f2179f92b
Windows XP(SP3, Home, Professional)	Option 55	37010f03062c2e2f1f21f92b
Windows Mobile	Option 60	3c4d6963726f736f66742057696e646f777320434500
Windows 7 Phone	Option 55	370103060f2c2e2f
Apple Mac OSX	Option 55	370103060f775ffc2c2e2f

Appendix B: Contacting Aruba Networks

Contacting Aruba Networks

Web Site Support	
Main Site	http://www.arubanetworks.com
Support Site	https://support.arubanetworks.com
Software Licensing Site	https://licensing.arubanetworks.com/login.php
Wireless Security Incident Response Team (WSIRT)	http://www.arubanetworks.com/support/wsirt.php
Support Emails	
Americas and APAC	support@arubanetworks.com
EMEA	emea_support@arubanetworks.com
WSIRT Email Please email details of any security problem found in an Aruba product.	wsirt@arubanetworks.com

Validated Reference Design Contact and User Forum	
Validated Reference Designs	http://www.arubanetworks.com/vrd
VRD Contact Email	referencedesign@arubanetworks.com
AirHeads Online User Forum	http://airheads.arubanetworks.com

Telephone Support	
Aruba Corporate	+1 (408) 227-4500
FAX	+1 (408) 227-4550
Support	
<ul style="list-style-type: none"> ● United States 	+1-800-WI-FI-LAN (800-943-4526)
<ul style="list-style-type: none"> ● Universal Free Phone Service Numbers (UIFN): 	
<ul style="list-style-type: none"> ■ Australia 	Reach: 1300 4 ARUBA (27822)
<ul style="list-style-type: none"> ■ United States 	1 800 9434526 1 650 3856589
<ul style="list-style-type: none"> ■ Canada 	1 800 9434526 1 650 3856589
<ul style="list-style-type: none"> ■ United Kingdom 	BT: 0 825 494 34526 MCL: 0 825 494 34526

Telephone Support

- Universal Free Phone Service Numbers (UIFN):

<ul style="list-style-type: none"> ■ Japan 	IDC: 10 810 494 34526 * Select fixed phones IDC: 0061 010 812 494 34526 * Any fixed, mobile & payphone KDD: 10 813 494 34526 * Select fixed phones JT: 10 815 494 34526 * Select fixed phones JT: 0041 010 816 494 34526 * Any fixed, mobile & payphone
<ul style="list-style-type: none"> ■ Korea 	DACOM: 2 819 494 34526 KT: 1 820 494 34526 ONSE: 8 821 494 34526
<ul style="list-style-type: none"> ■ Singapore 	Singapore Telecom: 1 822 494 34526
<ul style="list-style-type: none"> ■ Taiwan (U) 	CHT-I: 0 824 494 34526
<ul style="list-style-type: none"> ■ Belgium 	Belgacom: 0 827 494 34526
<ul style="list-style-type: none"> ■ Israel 	Bezeq: 14 807 494 34526 Barack ITC: 13 808 494 34526
<ul style="list-style-type: none"> ■ Ireland 	EIRCOM: 0 806 494 34526
<ul style="list-style-type: none"> ■ Hong Kong 	HKTI: 1 805 494 34526
<ul style="list-style-type: none"> ■ Germany 	Deutsche Telekom: 0 804 494 34526
<ul style="list-style-type: none"> ■ France 	France Telecom: 0 803 494 34526
<ul style="list-style-type: none"> ■ China (P) 	China Telecom South: 0 801 494 34526 China Netcom Group: 0 802 494 34526
<ul style="list-style-type: none"> ■ Saudi Arabia 	800 8445708
<ul style="list-style-type: none"> ■ UAE 	800 04416077
<ul style="list-style-type: none"> ■ Egypt 	2510-0200 8885177267 * within Cairo 02-2510-0200 8885177267 * outside Cairo
<ul style="list-style-type: none"> ■ India 	91 044 66768150