



DHCPv6 Fingerprinting and BYOD

Tom Coffeen, IPv6 Evangelist NAv6TF Summit 2013

- I. What is BYOD and why is it important?
- 2. What is DHCP(v6) fingerprinting?
- 3. How does DHCP fingerprinting works in IPv4?
- 4. Information about DHCP fingerprinting data
- 5. Benefit of DHCP(v6) fingerprinting
- 6. Differences in how DHCPv6 fingerprinting works
- 7. The potential value of building an open DHCPv6 fingerprint database



So, you've been living under a rock (or working for an SP)

BYOD is:

- a) The latest hip hop sensation from Slovenia (no cheating by asking Jan Z!)
- b) General Zod's little brother from the planet Krypton
- c) Line four on the eye chart
- d) An abbreviation for "bring your own device";
 i.e., end user personal devices on the corporate network



Why the BYOD challenge is coming to an enterprise near you



Source: Mary Meeker, Internet Trends @Stanford – Bases 12/03/2012



Why the BYOD challenge is coming to an enterprise near you



Source: Mary Meeker, Internet Trends @Stanford – Bases 12/03/2012



4,294,967,296 < 7,000,000,000



And why the BYOD challenge will include IPv6



Source: Geoff Huston IPv4 Address Report, 4/8/2013



What is DHCP(v6) fingerprinting?





The goal is to determine the client type using only data from a basic DHCP transaction



DHCP Transaction





DHCP Transaction





000		X Capturing from	n Standard input [Wires	hark 1.8.4 (SVN Re	Rev 46250 from /trunk-1.8)]	
<u>F</u> ile <u>E</u> di	it <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u>	nalyze <u>S</u> tatistics Te	elephony <u>T</u> ools <u>I</u> nt	ernals <u>H</u> elp		
	🎒 🎒 🕍 📄 🗔	🗙 🔁 📇 🔍	🔶 🗼 🥺 春 🚽		9. 이 예 🖭 🍑 🕅 🍢 💢	
Filter: i	р		▼ Expression C	Clear Apply S	Save	
No. T	ime	Source	Destination	Protocol Len	ngth Info	â
6 45	5.720692000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886	Sa 🛛
10 53	3.936244000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886	ŝa 🛛
11 61	1.497782000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886	ŝa 🛛
12 74	4.747047000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886	ŝa 🛛
13 88	8.182460000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886	3a
15 91	1.753487000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0xde90757	′5 🏹
4		<u> </u>		BU IOD		D
Maga	and type, Beet Beguest (1)				T
Hard Hard Hops Tran	dware type: Boot Request (dware type: Ethernet dware address length: 6 s: 0 nsaction ID: 0x94aa886a	1)				Î
Seco ▷ Boot Clie Your Next Rela Clie Clie Serv Boot Boot Magi ▷ Opti ▷ Opti ▷ Opti Padd	onds elapsed: 0 tp flags: 0x0000 (Unicast ent IP address: 0.0.0.0 (r (client) IP address: 0.0. ay agent IP address: 0.0. ent MAC address: CadmusCo ent hardware address padd ver host name not given t file name not given t file name not given t c cookie: DHCP Lon: (53) DHCP Message Ty Lon: (55) Parameter Reque Lon: (255) End ding) 0.0.0.0) 0.0.0 (0.0.0.0) 0.0 (0.0.0.0) _53:a4:fb (08:00:27:5 ing: 000000000000000000000000000000000000	53:a4:fb) 00000			Ţ
0000 ff	ff ff ff ff ff 08 00 27	53 a4 fb 08 00 45 10	E			
0010 01 0020 ff 0030 88 0040 00			i .H 9 aD.C.4 , D .j 'S			Q
🔘 💅 🛛 Fra	ame (frame), 342 bytes	Packets: 87 Displa	ayed: 37 Marked: 0		Profile: Default	



000)	X Capturing from	n Standard input [Wires	hark 1.8.4 (SVN Rev	/ 46250 from /trunk-1.8)]	
<u>F</u> ile <u>E</u>	<u>-</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u>	nalyze <u>S</u> tatistics To	elephony <u>T</u> ools <u>I</u> nt	ernals <u>H</u> elp		
e č	i 🔍 🈂 📦 🖿 🗔	X 2 🔒 🔍	🔶 📦 🤣 🐴 🛓		2, 0, 0, 🖭 🍑 🔟 ங % 💢	
Filter:	ip		▼ Expression C	Clear Apply Sav	ave	
No.	Time	Source	Destination	Protocol Lengt	gth Info	<u> </u>
6	45.720692000	0.0.0.0	255.255.255.255	DHCP 3	342 DHCP Discover - Transaction ID 0x94aa886a	U
10	53.936244000	0.0.0.0	255.255.255.255	DHCP 3	342 DHCP Discover - Transaction ID 0x94aa886a	
11	61.497782000	0.0.0.0	255.255.255.255	DHCP 3	342 DHCP Discover - Transaction ID 0x94aa886a	
12	74.747047000	0.0.0.0	255.255.255.255	DHCP 3	342 DHCP Discover - Transaction ID 0x94aa886a	
13	88.182460000	0.0.0.0	255.255.255.255	DHCP 3	342 DHCP Discover - Transaction ID 0x94aa886a	
15	91.753487000	0.0.0.0	255.255.255.255	DHCP 3	342 DHCP Discover - Transaction ID 0xde907575	¥
1		<u> </u>		<u></u>		
		2.)	,	*****		
Ha Ha Hoj Tri Sec Cl: Yoi Re Cl: Cl: Sec Boi Ma Dop Dop Pa	rdware type: Ethernet rdware address length: 6 ps: 0 ansaction ID: 0x94aa886a conds elapsed: 0 otp flags: 0x0000 (Unicast ient IP address: 0.0.0.0 (ur (client) IP address: 0.0. lay agent IP address: 0.0. lay agent IP address: 0.0. lay agent IP address: 0.0. ient MAC address: CadmusCo ient hardware address padd rver host name not given ot file name not given ot file name not given gic cookie: DHCP tion: (53) DHCP Message Ty tion: (55) Fand dding) 0.0.0.0) 0.0.0 (0.0.0.0) 0.0 (0.0.0.0) _53:a4:fb (08:00:27:5 ing: 000000000000000000000000000000000000	53:a4:fb) 00000			
0000	f ff ff ff ff ff 08 00 27	53 a4 fb 08 00 45 1	E	•		
0010 0 0020 f 0030 8 0040 0						U v
🔾 💆 F	rame (frame), 342 bytes	Packets: 87 Displa	ayed: 37 Marked: 0		Profile: Default	







000	X Capturing fro	m Standard input [Wires]	hark 1.8.4 (SVN F	Rev 46250 from /trunk-1	.8)]		
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>A</u> nalyze <u>S</u> tatistics T	elephony <u>T</u> ools <u>I</u> nte	ernals <u>H</u> elp				
🗐 🕍 🗐 🎱 📦 🖿 🔚		🗢 🗼 😜 ዥ 🚽		€ Q 🗓 🎹	🏹 🔟 🎦 💥		
Filter: ip		▼ Expression C	lear Apply	Save			
No. Time	Source	Destination	Protocol Le	ngth Info		<u> </u>	
6 45.720692000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x94aa	886a 🛛	
10 53.936244000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x94aa	886a	
11 61.497782000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x94aa	886a	
12 74.747047000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x94aa	886a	
13 88.182460000	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover	- Transaction ID 0x94aa	886a 🚽	
15 91 753487000	0000	255 255 255 255	DHCP	342 DHCP Discover	- Transaction ID Oxde90	7575	
Dontropt (52) DHCD Magazaga T	100						
✓ Option: (55) DHCP Message I	ype ost list					^	
Vopcion. (55) Parameter Requ	est List						
Deremeter Request List It	am. (1) Subpat Mask						
Darameter Request List It	em: (28) Broadcast Ac	drass					
Parameter Request List It	em: (2) Time Offset	0.035					
Parameter Request List It	em: (121) Classless 9	tatic Boute					
Parameter Request List It	em: (15) Domain Name						
Parameter Request List It	em: (6) Domain Name S	erver					
Parameter Request List It	em: (12) Host Name						
Parameter Request List It	em: (40) Network Info	rmation Service Domai	n				
Parameter Request List Item: (41) Network Information Service Servers							
Parameter Request List It	em: (42) Network Time	Protocol Servers					
Parameter Request List Item: (26) Interface MTU							
Parameter Request List It	em: (119) Domain Sear	ch [TODO:RFC3397]					
Parameter Request List It	em: (3) Router						
Parameter Request List It	em: (121) Classless S	tatic Route					
Parameter Request List It	em: (249) Private/Cla	ssless Static Route ((Microsoft)				
Parameter Request List It	em: (252) Private/Pro	xy autodiscovery					
Parameter Request List It	em: (42) Network Time	Protocol Servers				U	
▷ Option: (255) End						•	
0000 ff ff ff ff ff ff <u>08 00</u> 2	27 53 a4 fb 08 0 <u>0 45 1</u>	0					
0010 01 48 00 00 00 00 80 11 3		f .H 9					
0020 ff ff 00 44 00 43 01 34 2		aD.C.4 ,				U	
		0				•	
○ M Frame (frame) 342 bytes	Packets: 87 Displ	aved: 37 Marked: 0		Profile: Defaul	lt		
	1. denets, or Dispi	ajear of markedr o		4 Home Derau	is a second seco		



O O O X Capturing fro	om Standard input [Wires	hark 1.8.4 (SVI	N Rev 46250 from /trunk-1.8)]					
<u>File Edit V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics T	Telephony <u>T</u> ools <u>I</u> nt	ernals <u>H</u> elp						
			0, 0, 0, 17 🎬 🕅 🍢 💥 💢					
Filter: ip	Expression C	Clear Apply	Save					
No. Time Source	Destination	Protocol l	ength Info	1				
6 45.720692000 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886a					
10 53.936244000 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886a					
11 61.497782000 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886a					
12 74.747047000 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886a					
13 88.182460000 0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x94aa886a					
15 91 753487000 0.0.0.0	255 255 255 255	DHCP	342 DHCP Discover - Transaction ID Oxde907575	54				
			, ,					
V Option: (53) DHCP Messade IV6e		-		1				
✓ Option: (55) Parameter Request List								
Depember Dequest List Item: (1) Subpat Mask								
Parameter Request List Item: (1) Subnet Mask	danaca							
Parameter Request List Item: (2) Time Officet	uuress							
Parameter Request List Item: (121) Classless	Static Pouto							
Parameter Request List Item: (15) Domain Name								
Parameter Request List Item: (6) Domain Name Server								
Parameter Request List Item: (12) Host Name								
Parameter Request List Item: (12) Notwork Inf.	Parameter Request List Item: (40) Network Information Service Domain							
Parameter Request List Item: (4) Network Information Service Servers								
Parameter Request List Item: (42) Network Time Protocol Servers								
Parameter Request List Item: (42) Network Time Protocol Servers								
Parameter Request List Item: (20) Interface MIU Denameter Request List Item: (110) Demain Search [TODO:PEC2207]								
Darameter Request List Item: (3) Bouter								
Parameter Request List Item: (3) Noter	Static Boute							
Parameter Request List Item: (249) Private/(]	assless Static Boute	(Microsoft)						
Parameter Request List Item: (252) Private/Pri	assuess static route	(HECTOSOTE)						
Parameter Request List Item: (22) Network Tim	e Protocol Servers							
voption. (200) Enu				Ŧ				
0000 if if if if if if as an ar is at the open of the				-17				
0010 01 48 00 00 00 00 80 11 39 96 00 00 00 ff	ff .H 9			Ô				
0020 ff ff 00 44 00 43 01 34 2c f2 01 01 06 00 94 a	aaD.C.4 ,. <u>.</u>			U				
0030 88 6a 00 00 00 00 00 00 00 00 00 00 00 00 00	00 .j							
0040 00 00 00 00 00 00 08 00 27 53 a4 fb 00 00 00 0	00 'S		4	٣				
🔘 💇 Frame (frame), 342 bytes 🛛 🚦 Packets: 87 Disp	layed: 37 Marked: 0] Profile: Default	1				



Option 55: Parameter Request List

```
▽ Option: (55) Parameter Request List
    Length: 17
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (28) Broadcast Address
    Parameter Request List Item: (2) Time Offset
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (12) Host Name
    Parameter Request List Item: (40) Network Information Service Domain
    Parameter Request List Item: (41) Network Information Service Servers
    Parameter Request List Item: (42) Network Time Protocol Servers
    Parameter Request List Item: (26) Interface MTU
    Parameter Request List Item: (119) Domain Search [TODO:RFC3397]
    Parameter Request List Item: (3) Router
    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
    Parameter Request List Item: (42) Network Time Protocol Servers
```

1, 28, 2, 121, 15, 6, 12, 40, 41, 42, 26, 119, 3, 121, 249, 252, and 42



DHCP Fingerprint database



http://www.fingerbank.org



DHCP Fingerprint database

dhcp_fingerprints.conf (excerpt)

858	[os 512]
859	description=Fedora 14 based distro
860	fingerprints=< <eot< th=""></eot<>
861	1,28,2,121,15,6,12,40,41,42,26,119,3
862	EOT
863	
864	[os 513]
865	description=Chrome OS
866	fingerprints=< <eot< th=""></eot<>
867	1,121,33,3,6,12,15,26,28,51,54,58,59,119
868	EOT
869	
870	[os 514]
871	description=Fedora 15 or 16 based distro
872	fingerprints=< <eot< th=""></eot<>
873	1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42
874	EOT
875	
876	[os 515]
877	description=RHEL 6.4 or Centos6.4
878	fingerprints=< <eot< th=""></eot<>
879	1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,42
880	EOT
881	
882	[os 600]
883	description=Xbox
884	fingerprints=< <eot< th=""></eot<>
885	3,6
886	EOT



870	[os 514]
871	description=Fedora 15 or 16 based distro
872	fingerprints=< <eot< th=""></eot<>
873	1,28,2,121,15,6,12,40,41,42,26,119,3,121,249,252,42
874	EOT

















Linux fedoral7v6test 3.7.3-101.fc17.x86_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 > 86_64 x86_64 x86_64 GNU/Linux



DHCP Fingerprinting and BYOD





DHCP(v6) fingerprinting and BYOD

- Actionable data
 - Security
 - Captive portal approach allows device access or isolation
 - Reporting
 - What devices are connecting (or attempting to connect)?
- Passive -- no additional transactional overhead
 - compare with nmap host OS detection



DHCP Fingerprinting and BYOD

Infoblox HQ BYOD Day

- Tablets
- Smartphones
- Gaming consoles
- Home routers
- eReaders
- Desktops
- Over 78 unique devices identified
 - Software version learned for 81% of devices



Device	Operating System
Laptop (Window 7)	Professional Service pack Copyright @2009
Apple IPHONE	Version 6.0.1(10A523) Model MD237LL
MAC OS X	Version 10.7.4
MAC OS X	Version 10.5.8
Sony Xperia	AndroidVersion 4.0.4 KernelVersion 2.6.32.9-perf Model MT25I
Samsung Note II	AndroidVersion 4.1.1 KernelVersion 3.031-414933 Model SCH-1605
HTC Android	Version 4.0.4 S/W no - 2.35.531.10710rD HTC Sense Version - 4.1
iTouch	Version 6.1(10B141) Model MD724LL/A
iPhone	Version 6.1(10B143) Model MD638LL/A
iPad 4	Version 6.1(10B141)Â Model MD511LL/A
iPad 2	Version 6.0(10A403)Â Model MD328LL
NOOK Color	Version 1.4.3 Model BNRV200
Kindle	Version 7.2.3_user_2330720
Samsung Galaxy Nexus	Android Version 4.1.1 Kernel Version 3.0.31-g396c4df
ASUS Nexus 7	Android Version 4.2.2 Kernel Version 3.1.10-g05b777c
Apple iPhone 4S	Version 6.1(10B144) Model MC608LL/A
Etc	



How is DHCPv6 fingerprinting different?





Same goal (client type), this time with DHCPv6











Elle Edit View Ço Çapture Analyze Statistics Telephony Tools Internals Help No. Time Source Destination Protocol Length Info 86 536.637505000 fe80::a00:27ff:fe53::aff02::1:2 DHCPv6 114 Solicit XD: 0x6249ab CD: 0001000118d6Fb1308002753a4f Conternet Protocol Version 6, Src: fe80::a00:27ff:fe53::adfb (fe80::a00:27ff:fe53::adfb), Dst: ff02::1:2 (ff02::1:2) User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547) DHCPv6 Message type: Solicit (1) Transaction ID: 0x6249ab Colient Identifier (1) Length: 14 Value: 0001000118d6fb1308002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4fb Option: Option Request Option: Option Request (6) Length: 4 Value: 0010018 Requested Option code: DMS recursive name server (23) Requested Option code: DMS recursive name server (24) Value: 0000 el abased-time : 0 ms
No. Time Source Destination Protocol Length Info 06 536.63750000 f=800:1a00:27ff;f=53:ff02:11:2 PHCPv6 114 Solicit XID: 0xc249ab CID: 0001000118d0fb1308002753a4f 1 Internet Protocol Version 6, Src: fe80::a00:27ff;f=53:a4fb (fe80::a00:27ff;f=53:a4fb), Dst: ff02::1:2 (ff02::1:2) > > User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547) > > DHCPv6 Message type: Solicit (1) Transaction ID: 0x6249ab Client Identifier: 0001000118d0fb1308002753a4fb > Option: Client Identifier (1) Length: 14 value: 0001000118d0fb1308002753a4fb > DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:2:07 POT Link-layer address: 08:00:27:53:a4fb Client Request (6) Length: 4 value: 0017018 Requested Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) Value: 0000 elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed time 0 ms
<pre>S 356.637505000 fe80::a00:27ff:fe53:4ff02::1:2 0HCPv6 111 Solicit XID: 0x6249ab CID: 0001000118doff1506002753.4ff</pre>
<pre>Internet if, pre: dumance_port.retroord://pre:/fiestiate/port.com/comparison/compa</pre>
<pre>> Internet Protocol Version 6, Src: fe80::a00:27ff:fe53:a4fb (fe80::a00:27ff:fe53:a4fb), Dst: ff02::l:2 (ff02::l:2) >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>
<pre>p Internet Protocol Version 6, Src: fe80::a00:27ft:fe53:a4fb (fe80::a00:27ff:fe53:a4fb), Dst: ff02::1:2 (ff02::1:2) User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547) Message type: Solicit (1) Transaction ID: 0x6249ab Client Identifier: 0001000118d0fb1308002753a4fb Option: Client Identifier (1) Length: 14 Value: 0001000118d0fb1308002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb Option: Option Request (6) Length: 4 Value: 00170018 Request (6) Length: 4 Value: 00170018 Request (6) Length: 4 Value: 00170018 Request Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) Value: 001000 Value: 0000 elapsed time (8) Length: 2 Value: 0000 elapsed time: 0 mms </pre>
<pre>publicity by by</pre>
<pre>Message type: Solicit (1) Transaction ID: 0x6249ab Client Identifier: 0001000118d0fb1308002753a4fb Option: Client Identifier (1) Length: 14 Value: 0001000118d0fb1308002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb Option: Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (24) </pre>
Transaction ID: 0x6249ab V Client Identifier: 0001000118d0fb1308002753a4fb Option: Client Identifier (1) Length: 14 Value: 0001000118d0fb1308002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb V Option Request Option Request Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (23) Requested Ime Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
<pre> Client Identifier: 0001000118d0fb1308002753a4fb Option: Client Identifier (1) Length: 14 Value: 0001000118d0fb1308002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Imme Option: Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed time: 0 ms </pre>
Option: Client Identifier (1) Length: 14 Value: 0001000118d0fb13008002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb ♥ Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ♥ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Length: 14 Value: 0001000118dofb1308002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb ♥ Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (23) Velapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
<pre>Value: 0001000118dofb1308002753a4fb DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb ♥ Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ♥ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms</pre>
DUID type: link-layer address plus time (1) Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb ♥ Option Request Option Request Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ♥ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Hardware type: Ethernet (1) Time: Mar 11, 2013 13:29:07 PDT Link-layer address: 08:00:27:53:a4:fb ♥ Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ♥ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Link-layer address: 08:00:27:53:a4:fb V Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) V Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
<pre>> Option Request Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) > Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms</pre>
Option: Option Request (6) Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ▼ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Length: 4 Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ▼ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Value: 00170018 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ▼ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) ▼ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Requested Option code: Domain Search List (24) ▼ Elapsed time Option: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
<pre></pre>
Uption: Elapsed time (8) Length: 2 Value: 0000 elapsed-time: 0 ms
Value: 0000 elapsed-time: 0 ms
elapsed-time: 0 ms
▽ Identity Association for Non-temporary Address
Option: Identity Association for Non-temporary Address (3)
Length: 12
Value: 2753a4fb00000e1000001518
IAID: 2753a4fb
12: 5400
0000 33 33 00 01 00 02 08 00 27 53 a4 tb 86 dd 60 00 33 'S'.
0020 27 ff fe 53 a4 fb ff 02 00 00 00 00 00 00 00 00 'S
0030 00 00 01 00 02 02 22 02 23 00 3c 05 42 01 62".#.<.B.b



00	0	X C	apturing from Sta	andard input [Wire	shark 1.8.4 (SVN F	Rev 46250 from /trun	k-1.8)]	
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture	<u>A</u> nalyze <u>S</u> ta	atistics Telep	hony <u>T</u> ools <u>I</u> n	ternals <u>H</u> elp			
No	Time	Source		stination	Protocolla	nath		
110.		13001 Ce	2766.652.666			lla colicit VID	avenue- cro.	
8		f-00::a00:	2711:1053:2110	2::1:2	DHCPV6	114 Solicit XID:	0x6249ab CID:	0001000118d01b1308002753a41
•)+
D Int	ernet Protocol Version 6	Src: fe80a	00.27ff.fe53	a4fb (fe80a00.	27ff·fe53·e4fh)	Det. ff021.2	., (ff021.2)	2
D Use	r Datagram Protocol. Src P	ort: dhcpv6-	client (546).	Dst Port: dhcpv	6-server (547)	, DSC. 1102	(1102.11.2)	
	Pv6		,					1
N	essage type: Solicit (1)							
T	ransaction ID: 0x6249ab							
	lient Identifier: 00010001	18d0fb130800	02753a4fb					
	Option: Client Identifier	~ (1)						
	Length: 14							
	DUID type: lipk-laver ad	ress plus to	ime (1)					
	Hardware type: Ethernet	(1)	IIIIe (I)					
	Time: Mar 11, 2013 13:29	07 PDT						
	Link-layer address: 08:00	0:27:53:a4:ft	b					
~ (ption Request							
	Option: Option Request (6	5)						
	Length: 4							
	Value: 00170018		,					
	Requested Option code: Dr	NS recursive	hame server ((23)				
	Requested Option code: Do	main Search	LISU (24)					
	Option: Flapsed time (8)							
	Length: 2							
	Value: 0000							
	elapsed-time: O ms							
▼ 1	dentity Association for No	n-temporary	Address					
	Option: Identity Associat	tion for Non-	-temporary Add	lress (3)				
	Length: 12							
	Value: 2753a4tb00000e1000	0001518						
	IAID: 2/53a4Tb							
	T2: 5400							
0000		7 52 al fb	and the an					
0010			86 dd 60 00 00 00 0a 00					
0020			00 00 00 00					Ļ
0030			05 42 01 62 fb 13 08 00		b			



IPv4 DHCP Option Request (Option 55)



DHCPv6 Option Request (Option 6)

- Typically, fewer options appear under Option 6 in a DHCPv6 SOLICIT
- Other elements may be required to validate the device type or system
 - Vendor Class field (where present)
 - Timing how often the client sends a SOLICIT message
 - In dual-stack environments, correlation with the IPv4 fingerprint
 - The Client Identifier field in a DHCPv6 SOLICIT











DHCPv6 Fingerprints



- Currently, 198 unique fingerprints for DHCP
- None for DHCPv6
 - Likely due to a lack of general IPv6 deployment in environments where fingerprinting is potentially most useful (i.e., enterprise/corporate networks)
 - Thus, BYOD not generally a challenge for IPv6 (yet...)



DHCPv6 Fingerprints



- Collaborating with UNH-IOL on a public DHCPv6 fingerprint database
 - Benefits
 - IPv6 feature parity for a durably useful feature in IPv4
 - Increases the likelihood that the greatest number of devices will be accurately identified over time
 - May encourage the deployment of DHCPv6
 - May encourage effective BYOD policy







Questions?

tcoffeen@infoblox.com twitter: @ipv6tom

© 2013 Infoblox Inc. All Rights Reserved. 40

References

- <u>2012 Internet Trends</u>, Mary Meeker (KPCB), Dec. 2012
 - <u>http://www.kpcb.com/insights/2012-internet-trends</u>
- IPv4 Address Report, Geoff Huston (APNIC), Mar. 2013
 - <u>http://www.potaroo.net/tools/ipv4/</u>
- <u>Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315</u>, IETF, Jul. 2003
- Dynamic Host Configuration Protocol, RFC 2131, IETF, Mar. 1997
- <u>Chatter on the Wire: A look at DHCPv6 traffic</u>, by Eric Kollmann, Nov.
 2010
 - <u>http://chatteronthewire.org/download/chatter-dhcpv6.pdf</u>

