

# DHCPv6 Fingerprinting and BYOD

Tom Coffeen, IPv6 Evangelist  
NANOG 59 - Chandler, Arizona

# Agenda

---

1. 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

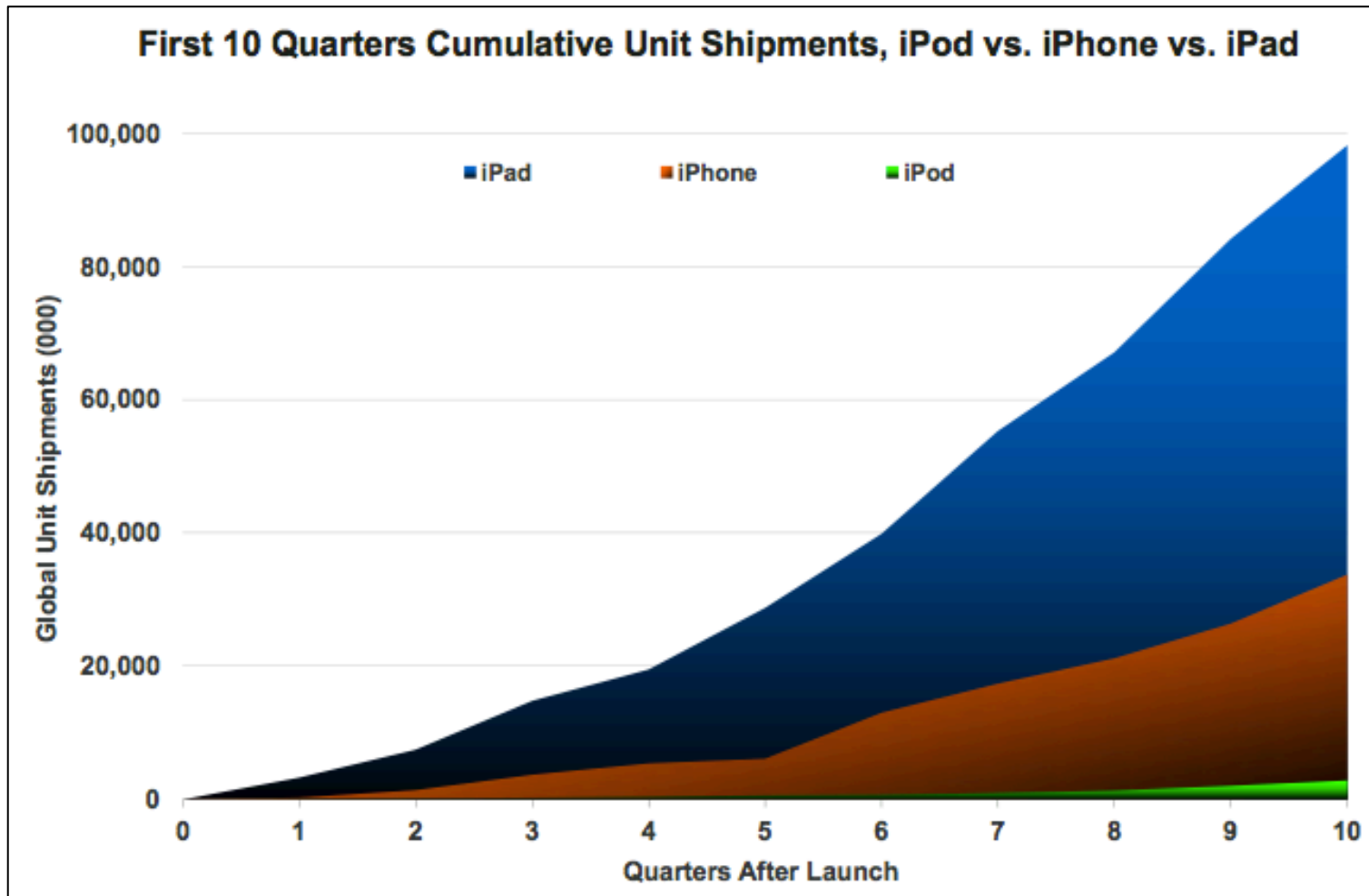
So, you've been living under a rock (or working for an SP)

---

BYOD is:

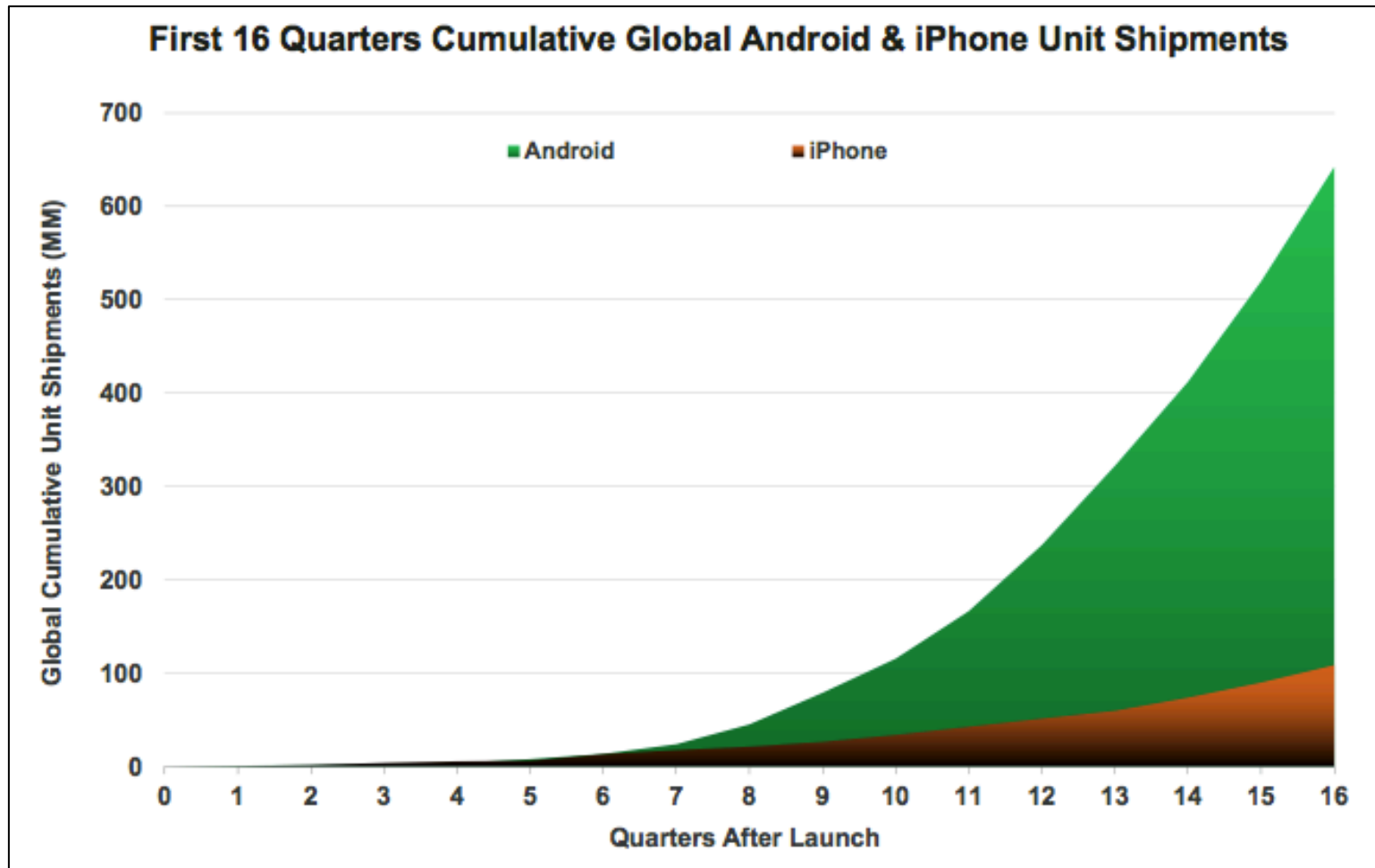
- a) The latest hip hop sensation from Slovenia
- b) General Zod's little brother from the planet Krypton
- c) Line four on the eye chart
- d) An abbreviation for “bring your own device”;  
i.e., end user personal devices on the  
corporate network

# 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

## What does massive device proliferation look like?

---

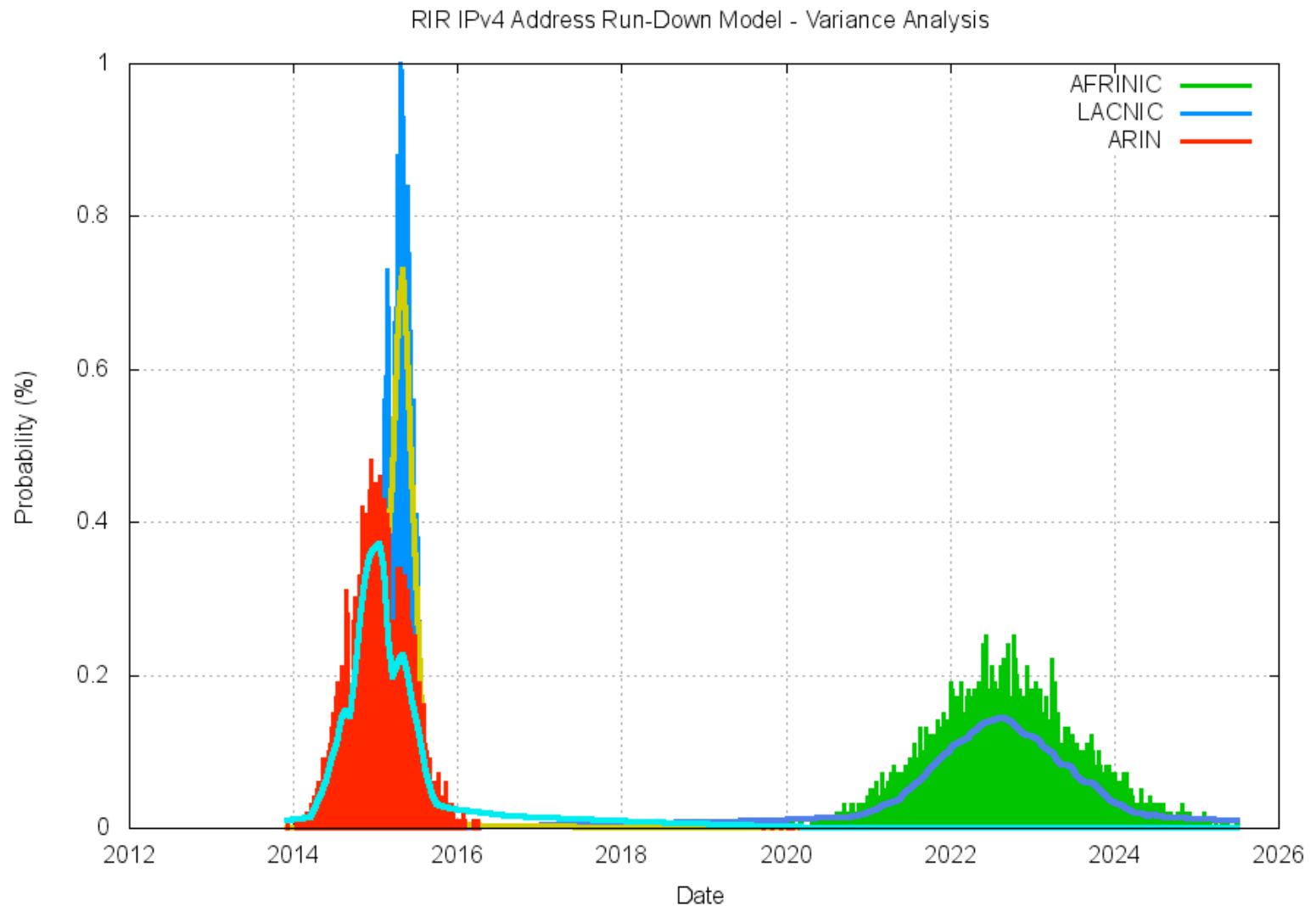


This slide is awesome

---

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

## And why the BYOD challenge will include IPv6



Source: Geoff Huston IPv4 Address Report, 9/24/2013



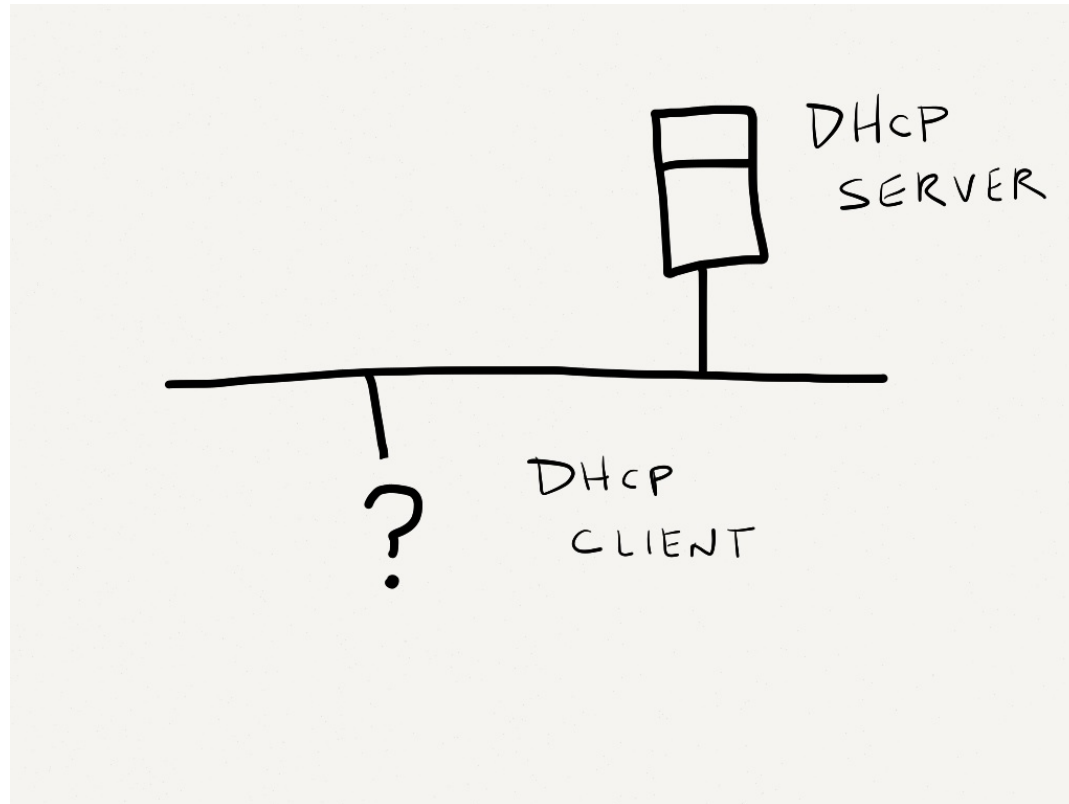
# DHCP Fingerprinting

---

What is DHCP fingerprinting?

# DHCP Fingerprinting

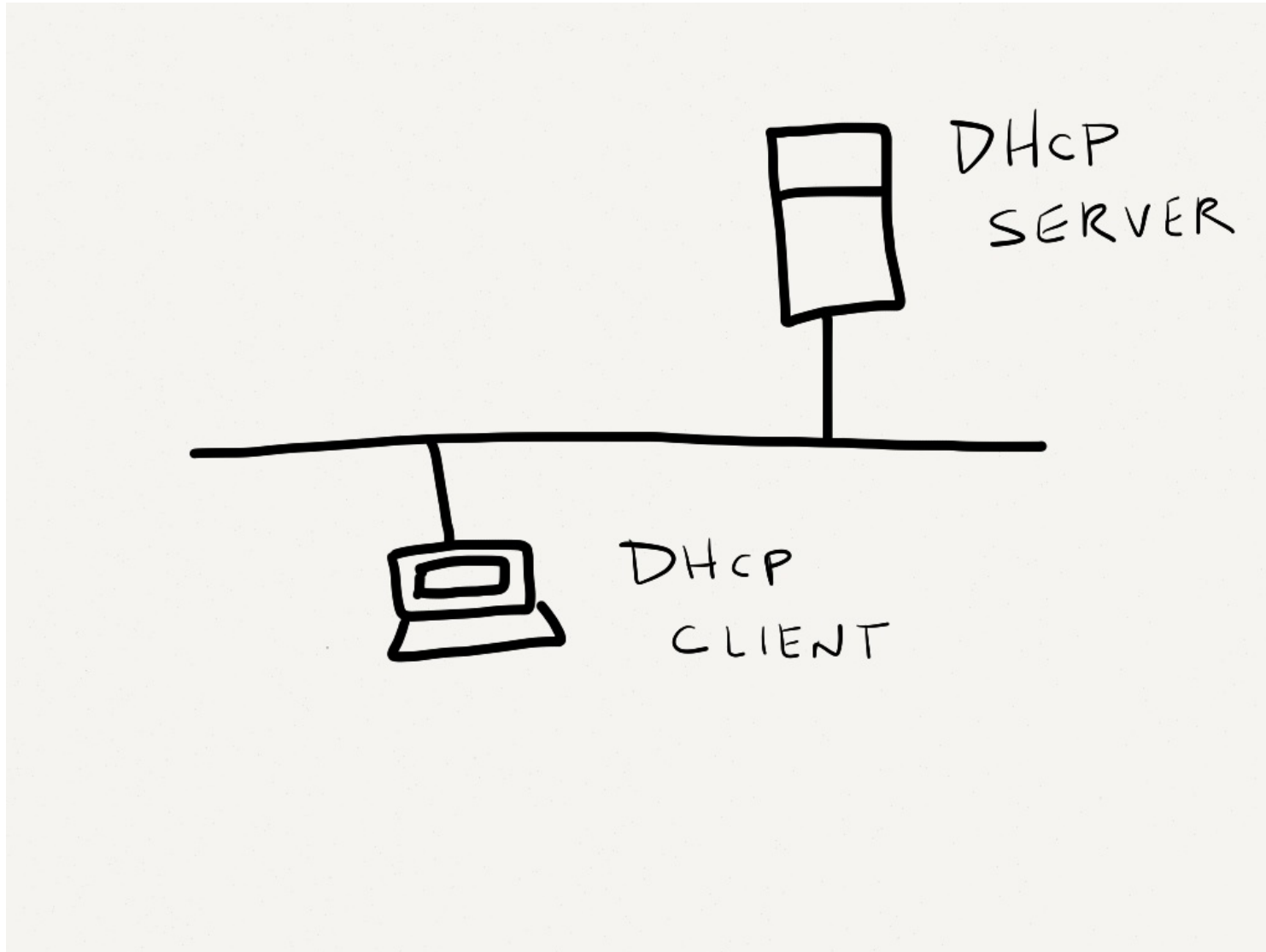
---



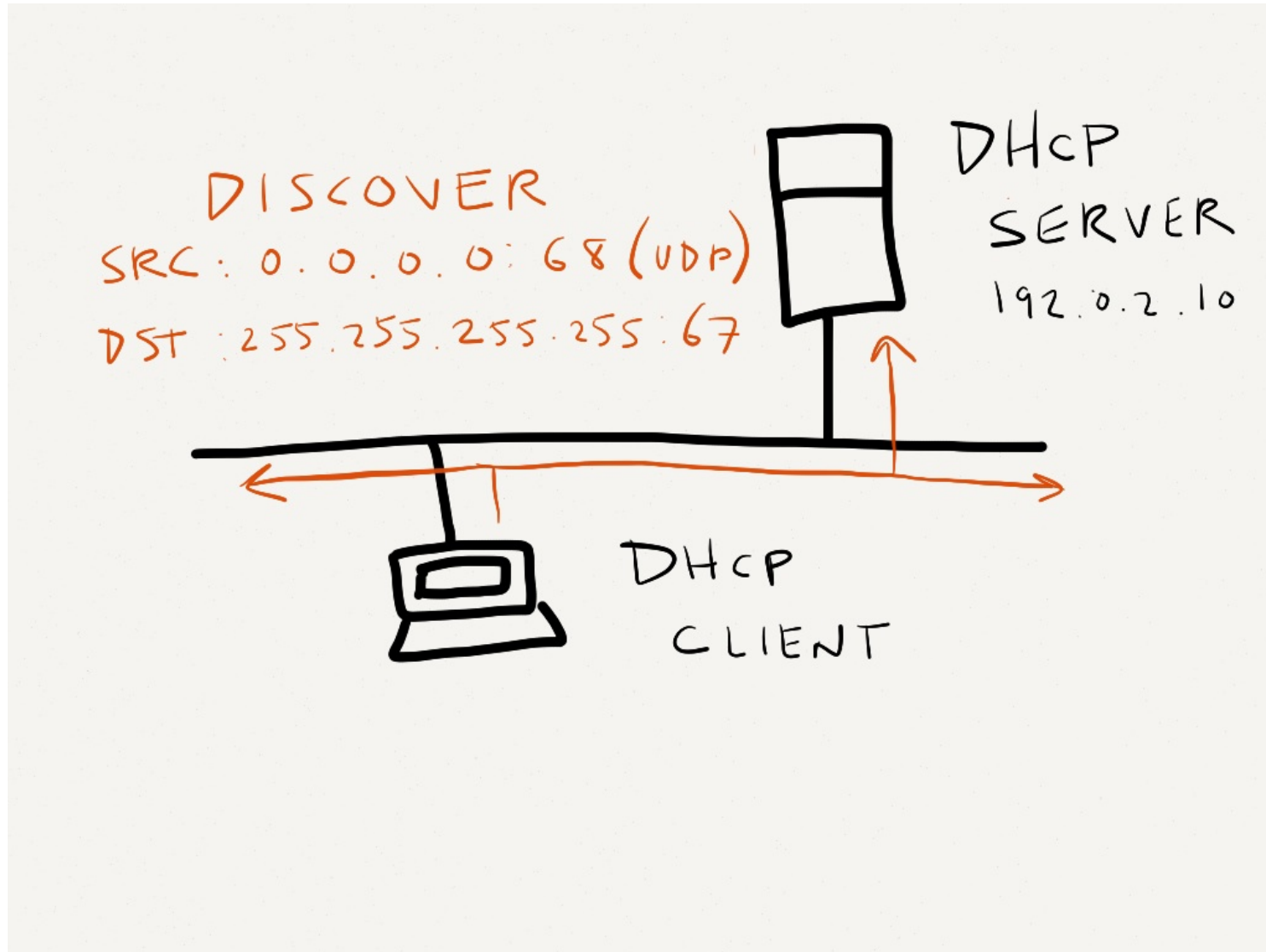
The goal is to determine the client type using only data from a basic DHCP transaction

# DHCP Transaction

---



# DHCP Transaction



# DHCP Fingerprinting

Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8) - Capturing from Standard input

Filter: **ip** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
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 0xde907575

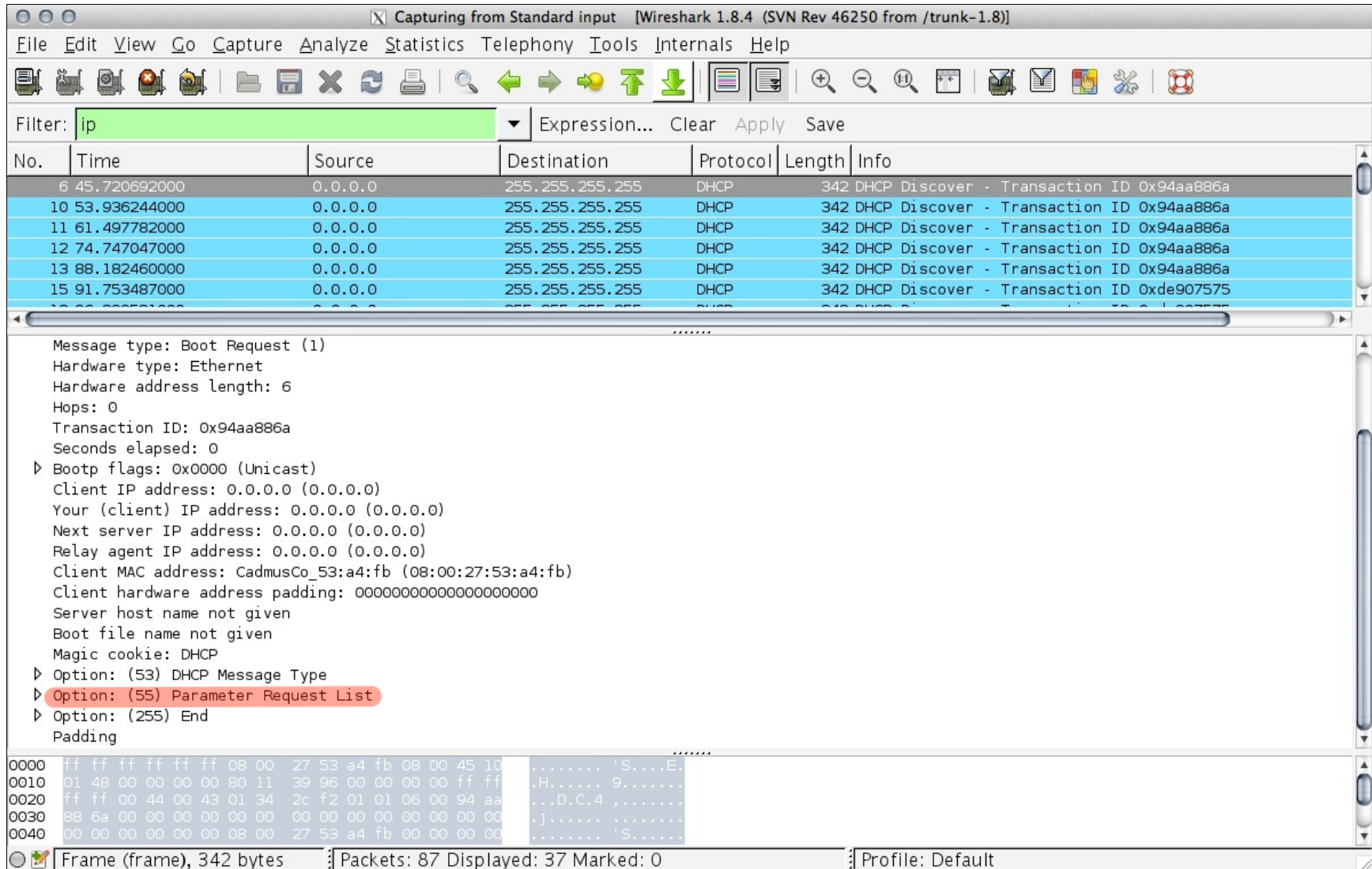
Message type: Boot Request (1)  
Hardware type: Ethernet  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0x94aa886a  
Seconds elapsed: 0

- ▶ Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0 (0.0.0.0)  
Your (client) IP address: 0.0.0.0 (0.0.0.0)  
Next server IP address: 0.0.0.0 (0.0.0.0)  
Relay agent IP address: 0.0.0.0 (0.0.0.0)  
Client MAC address: CadmusCo\_53:a4:fb (08:00:27:53:a4:fb)  
Client hardware address padding: 000000000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP
- ▶ Option: (53) DHCP Message Type
- ▶ Option: (55) Parameter Request List
- ▶ Option: (255) End  
Padding

0000 ff ff ff ff ff ff 08 00 27 53 a4 fb 08 00 45 10 ..... 'S....E.  
0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff ..H..... 9.....  
0020 ff ff 00 44 00 43 01 34 2c f2 01 01 06 00 94 aa ...D.C.4 .....  
0030 88 6a 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 00 ..... 'S.....

Frame (frame), 342 bytes | Packets: 87 Displayed: 37 Marked: 0 | Profile: Default

# DHCP Fingerprinting



Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8) - Capturing from Standard input

Filter: **ip** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
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 0xde907575

Message type: Boot Request (1)  
Hardware type: Ethernet  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0x94aa886a  
Seconds elapsed: 0

- ▶ Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0 (0.0.0.0)  
Your (client) IP address: 0.0.0.0 (0.0.0.0)  
Next server IP address: 0.0.0.0 (0.0.0.0)  
Relay agent IP address: 0.0.0.0 (0.0.0.0)  
Client MAC address: CadmusCo\_53:a4:fb (08:00:27:53:a4:fb)  
Client hardware address padding: 00000000000000000000
- Server host name not given  
Boot file name not given  
Magic cookie: DHCP
- ▶ Option: (53) DHCP Message Type
- ▶ Option: (55) Parameter Request List
- ▶ Option: (255) End  
Padding

0000 ff ff ff ff ff ff 08 00 27 53 a4 fb 08 00 45 10 ..... 'S....E.  
0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff ..H..... 9.....  
0020 ff ff 00 44 00 43 01 34 2c f2 01 01 06 00 94 aa ...D.C.4 .....  
0030 88 6a 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 00 ..... 'S.....

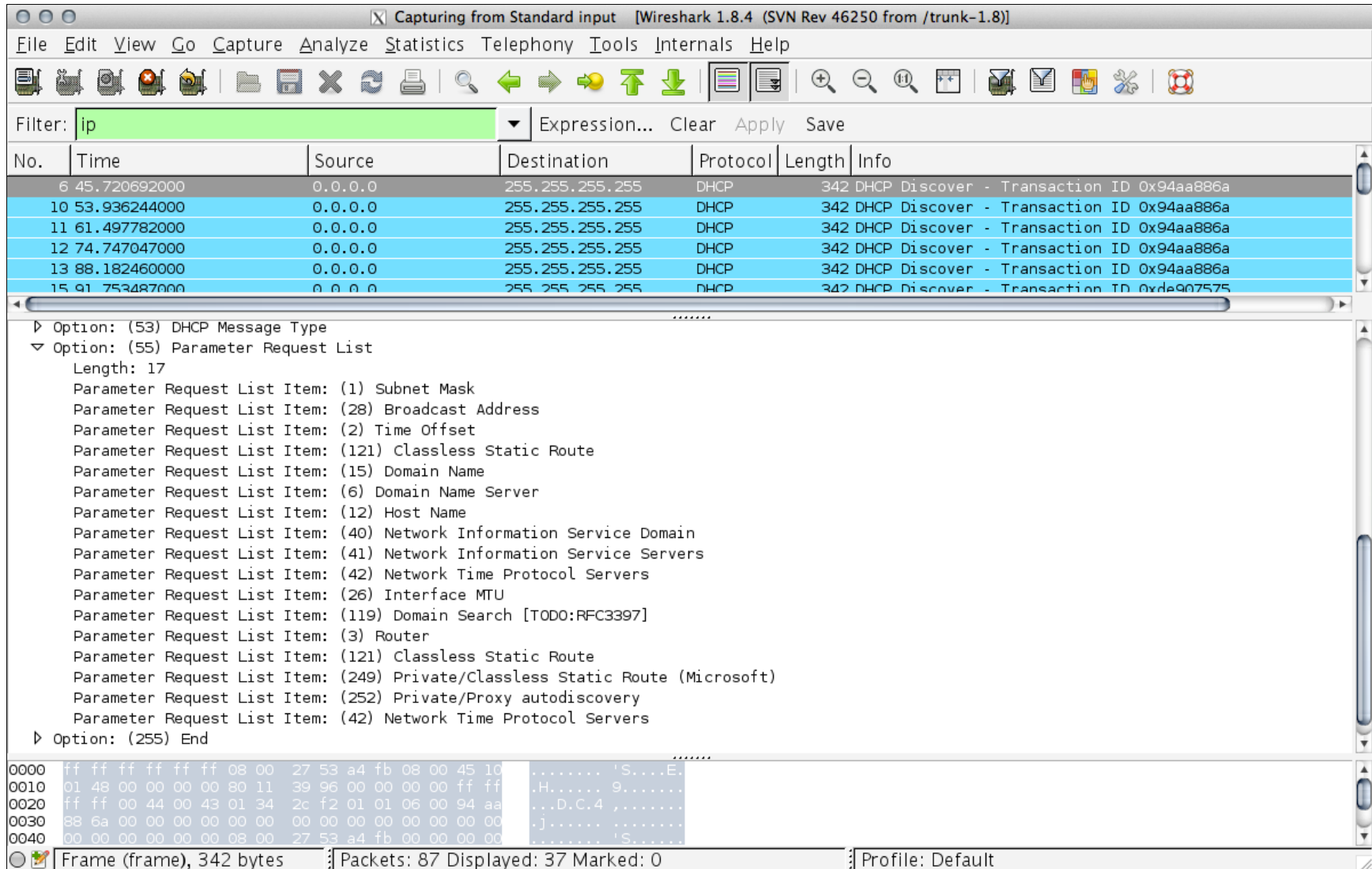
Frame (frame), 342 bytes | Packets: 87 Displayed: 37 Marked: 0 | Profile: Default

# DHCP Fingerprinting

---

▶ Option: (55) Parameter Request List

# DHCP Fingerprinting



Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)

Filter: **ip** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
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 0xda907575

Option: (53) DHCP Message Type

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

Option: (255) End

0000 ff ff ff ff ff ff 08 00 27 53 a4 fb 08 00 45 10 ..... 'S....E.

0010 01 48 00 00 00 00 80 11 39 96 00 00 00 00 ff ff ..H..... 9.....

0020 ff ff 00 44 00 43 01 34 2c f2 01 01 06 00 94 aa ...D.C.4 ,.....

0030 88 6a 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 00 ..... 'S.....

Frame (frame), 342 bytes | Packets: 87 Displayed: 37 Marked: 0 | Profile: Default



# DHCP Fingerprinting

The screenshot shows the Wireshark 1.8.4 interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter bar shows 'ip' selected. The packet list pane displays several DHCP Discover packets from source 0.0.0.0 to destination 255.255.255.255, all with Transaction ID 0x94aa886a. The packet details pane shows the selected packet's structure: Ethernet II, Internet Protocol Version 4, and DHCP. The DHCP section is expanded, showing Option (53) DHCP Message Type and Option (55) Parameter Request List. The Parameter Request List is highlighted with a red box and contains the following items:

- 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

The packet bytes pane at the bottom shows the raw data for the selected packet, with a hex dump and ASCII representation.

# DHCP Fingerprinting

## ■ 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
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
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
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
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
885 3,6
886 EOT
```

# DHCP Fingerprint database

---

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

# DHCP Fingerprinting

---



=

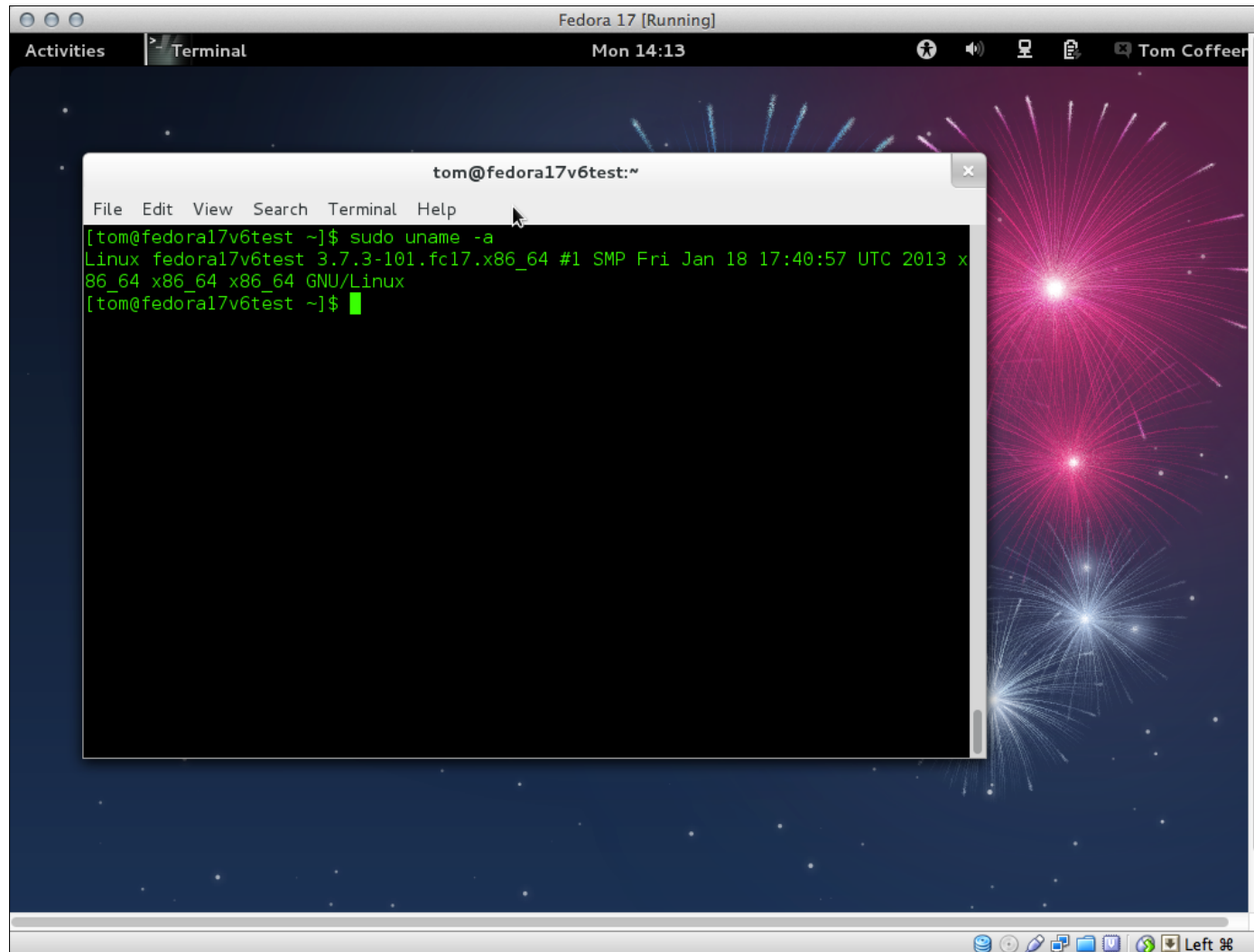
Option 55:  
1, 28, 2, 121,  
15, 6, 12, 40,  
41, 42, 26,  
119, 3, 121,  
249, 252,  
and 42

=



Fedora 17

# DHCP Fingerprinting

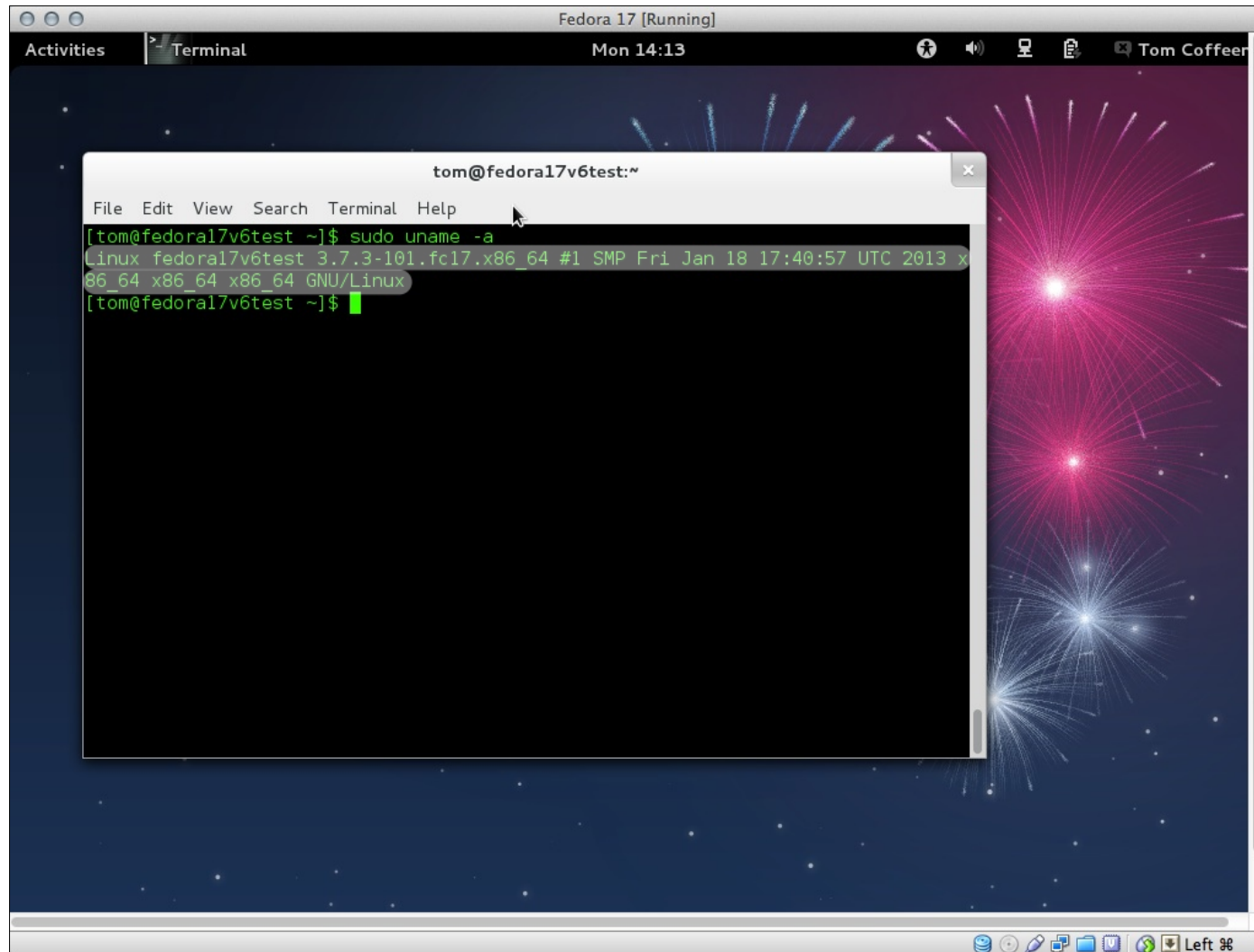


The screenshot shows a Fedora 17 desktop environment. The background is a dark blue night sky with white stars and several bright, colorful fireworks (pink, purple, and white) exploding on the right side. The desktop has a top panel with the title 'Fedora 17 [Running]' and a clock showing 'Mon 14:13'. Below the top panel is a menu bar with 'Activities' and 'Terminal'. A terminal window is open, displaying the command 'sudo uname -a' and its output. The terminal window has a title bar 'tom@fedora17v6test:~' and a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The output of the command is as follows:

```
[tom@fedora17v6test ~]$ sudo uname -a
Linux fedora17v6test 3.7.3-101.fc17.x86_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 x
86_64 x86_64 x86_64 GNU/Linux
[tom@fedora17v6test ~]$
```



# DHCP Fingerprinting



The screenshot shows a Fedora 17 desktop environment. The background is a dark blue night sky with white stars and colorful fireworks. A terminal window titled "tom@fedora17v6test:~" is open, displaying the output of the command "sudo uname -a". The output is: "Linux fedora17v6test 3.7.3-101.fc17.x86\_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 x86\_64 x86\_64 x86\_64 GNU/Linux". The terminal window has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The desktop has a top panel with "Activities", "Terminal", and "Mon 14:13". The bottom panel shows various system icons and a "Left" button.

```
tom@fedora17v6test:~  
File Edit View Search Terminal Help  
[tom@fedora17v6test ~]$ sudo uname -a  
Linux fedora17v6test 3.7.3-101.fc17.x86_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 x  
86_64 x86_64 x86_64 GNU/Linux  
[tom@fedora17v6test ~]$
```



# DHCP Fingerprinting

---

```
Linux fedora17v6test 3.7.3-101.fc17.x86_64 #1 SMP Fri Jan 18 17:40:57 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux
```

# DHCP Fingerprinting and BYOD

---



# DHCP/DHCPv6 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

# DHCP Fingerprinting

Device	Operating System
Laptop (Window 7)	Professional Service pack 1 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-I605
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) Model MD511LL/A
iPad 2	Version 6.0(10A403) Model MD328LL
NOOK Color	Version 1.4.3 Model BNRV200
Kindle	Version 7.2.3_user_2330720
Samsung Galaxy Nexus	AndroidVersion 4.1.1 KernelVersion 3.0.31-g396c4df
ASUS Nexus 7	AndroidVersion 4.2.2 KernelVersion 3.1.10-g05b777c
Apple iPhone 4S	Version 6.1(10B144) Model MC608LL/A
Etc...	

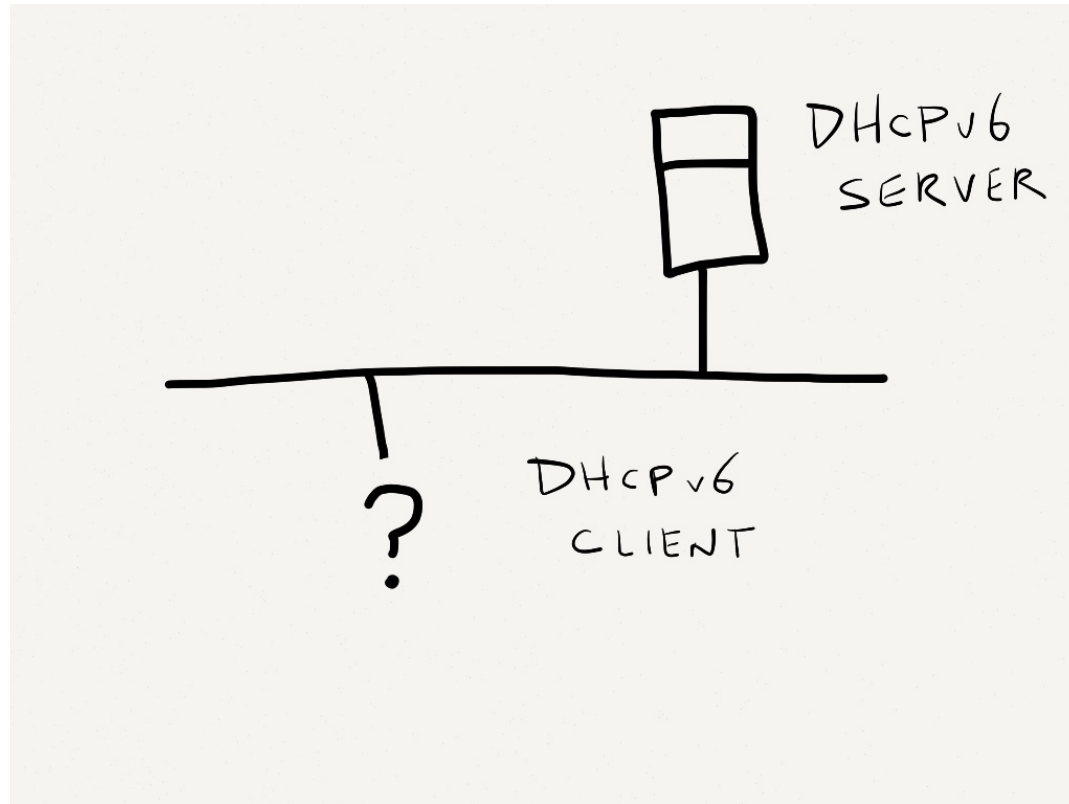
# DHCPv6 Fingerprinting

---

How is DHCPv6 fingerprinting different?

# DHCPv6 Fingerprinting

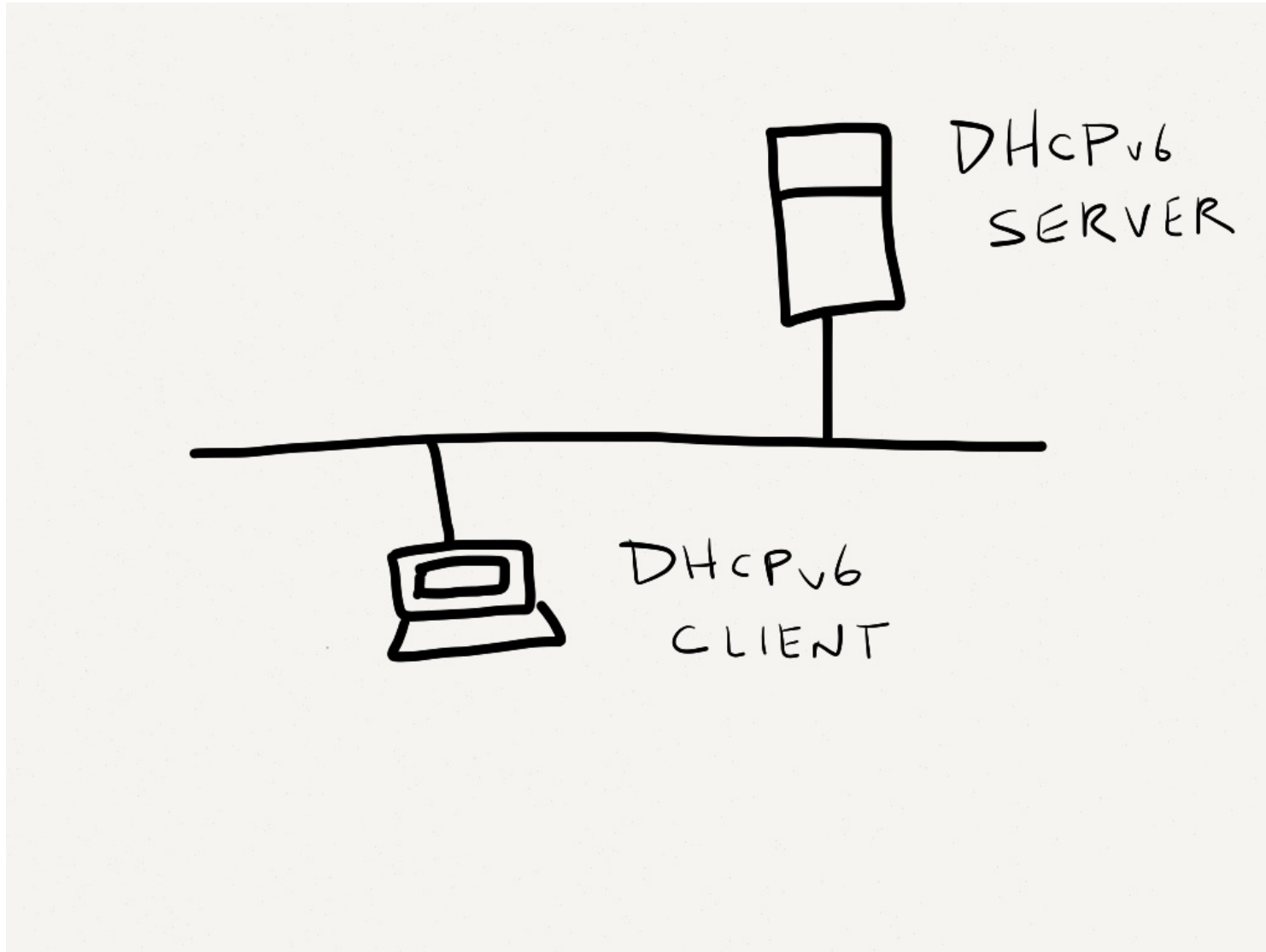
---



Same goal (client type), this time with DHCPv6

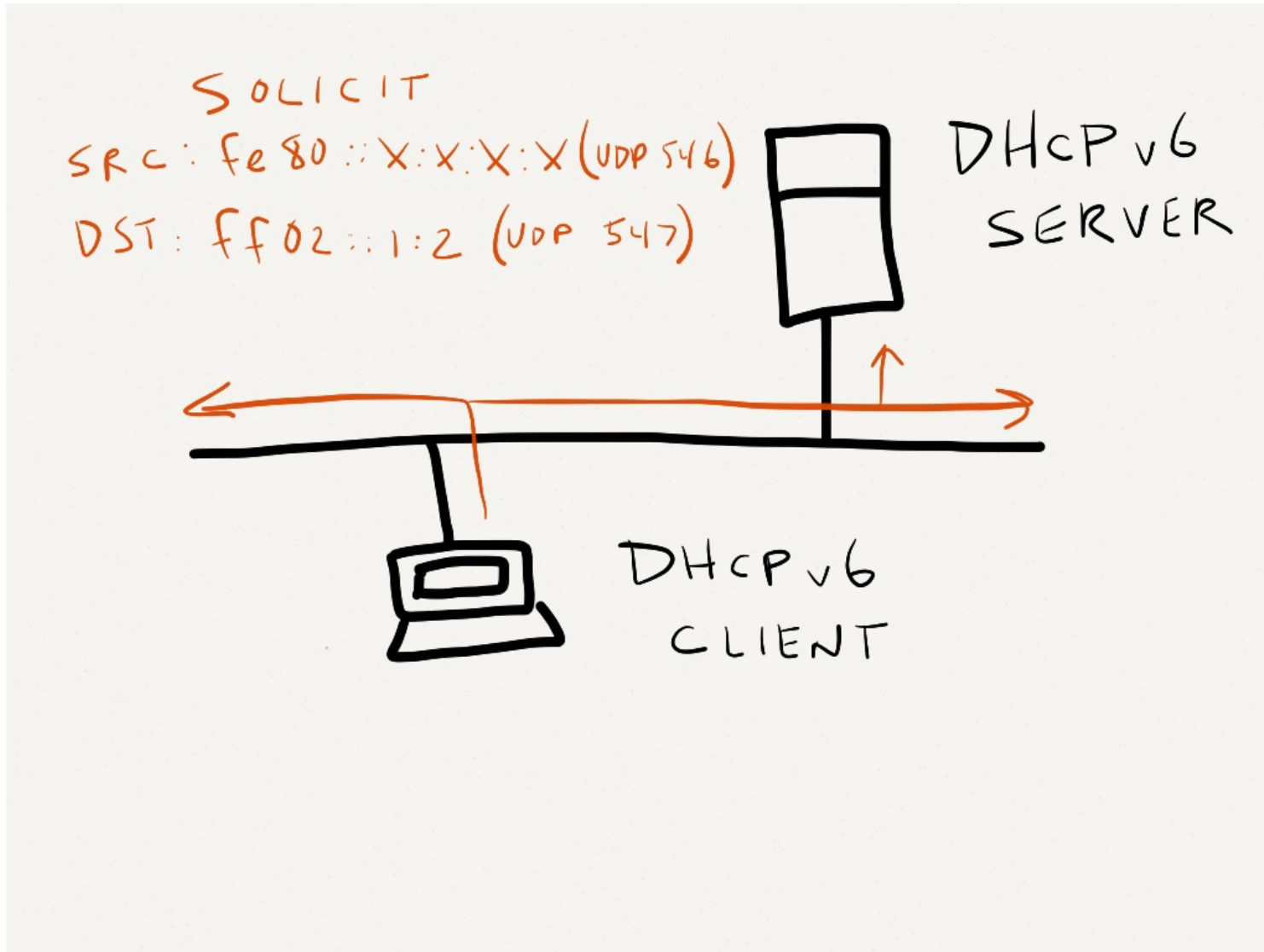
# DHCPv6 Fingerprinting

---





# DHCPv6 Fingerprinting



# DHCPv6 Fingerprinting

Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

No.	Time	Source	Destination	Protocol	Length	Info
86	536.637505000	fe80::a00:27ff:fe53:a4fb	ff02::1:2	DHCPv6	114	Solicit XID: 0x6249ab CID: 0001000118d0fb1308002753a4fb

Internet Protocol Version 6, Src: fe80::a00:27ff: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)

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 13:29:07 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
- Identity Association for Non-temporary Address
  - Option: Identity Association for Non-temporary Address (3)
  - Length: 12
  - Value: 2753a4fb000000e1000001518
  - IAID: 2753a4fb
  - T1: 3600
  - T2: 5400

0000 33 33 00 01 00 02 08 00 27 53 a4 fb 86 dd 60 00 33.....'S....  
0010 00 00 00 3c 11 01 fe 80 00 00 00 00 00 00 0a 00 ...<.....  
0020 27 ff fe 53 a4 fb ff 02 00 00 00 00 00 00 00 00 .....'.S.....  
0030 00 00 00 01 00 02 02 22 02 23 00 3c 05 42 01 62 .....".#.<.B.b  
0040 49 ab 00 01 00 0e 00 01 00 01 18 d0 fb 13 08 00 .....I.....

# DHCPv6 Fingerprinting

The image shows a Wireshark 1.8.4 capture of a DHCPv6 Solicit message. The packet list at the top shows a packet of length 114 bytes. The packet details pane on the right shows the following structure:

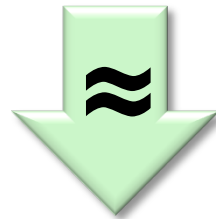
- Message type: Solicit (1)
- Transaction ID: 0x6249ab
- Client Identifier: 0001000118d0fb1308002753a4fb
  - Option: Client Identifier (1)
    - Length: 14
    - Value: 0001000118d0fb1308002753a4fb
    - DUID type: link-layer address plus time (1)
    - Hardware type: Ethernet (1)
    - Time: Mar 11, 2013 13:29:07 PDT
    - Link-layer address: 08:00:27:53:a4:fb
- Option 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
- Identity Association for Non-temporary Address
  - Option: Identity Association for Non-temporary Address (3)
    - Length: 12
    - Value: 2753a4fb000000e1000001518
    - IAID: 2753a4fb
    - T1: 3600
    - T2: 5400

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

# DHCPv6 Fingerprinting

---

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 Fingerprinting

```
▼ 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 13:29:07 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
  ▼ Identity Association for Non-temporary Address
    Option: Identity Association for Non-temporary Address (3)
```

# DHCPv6 Fingerprinting

---



=

SOLICIT, 1,  
6, 23, 24, 8,  
and 3

=



Fedora 17

# 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](mailto:tcoffeen@infoblox.com)

twitter: [@ipv6tom](https://twitter.com/ipv6tom)

# References

---

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