BLOX FEST

Infoblox

Robert Nagy

CEO – DeepDive Networking
rob@deepdivenetworking.com
www.deepdivenetworking.com

Topics Covered

- DHCP Fingerprinting
- Using Lease-History
- DDNS and Option-81

Insert Transition Slide – DHCP Fingerprinting

DHCP Fingerprinting

Overview

1,15,3,6,44,46,47,31,33,249,43
1,15,3,6,44,46,47,31,33,249,43,252
1,15,3,6,44,46,47,31,33,249,43,252,12
15,3,6,44,46,47,31,33,249,43
15,3,6,44,46,47,31,33,249,43,252
28,2,3,15,6,12,44,47

1,3,6,15,119,78,79,95,252
1,3,6,15,119,95,252,44,46,47

Who am I?

DHCP Fingerprinting

How it works

- MAC address gives us limited information
- Client often provides information about its OS and device type.
- The combination of the option sequence or vendor client ID in option 55 or 60 is used to infer the OS and device type of the remote client.
- These parameters are then incorporated into a DHCP fingerprint that provides unique information about this client.

DHCP Fingerprinting

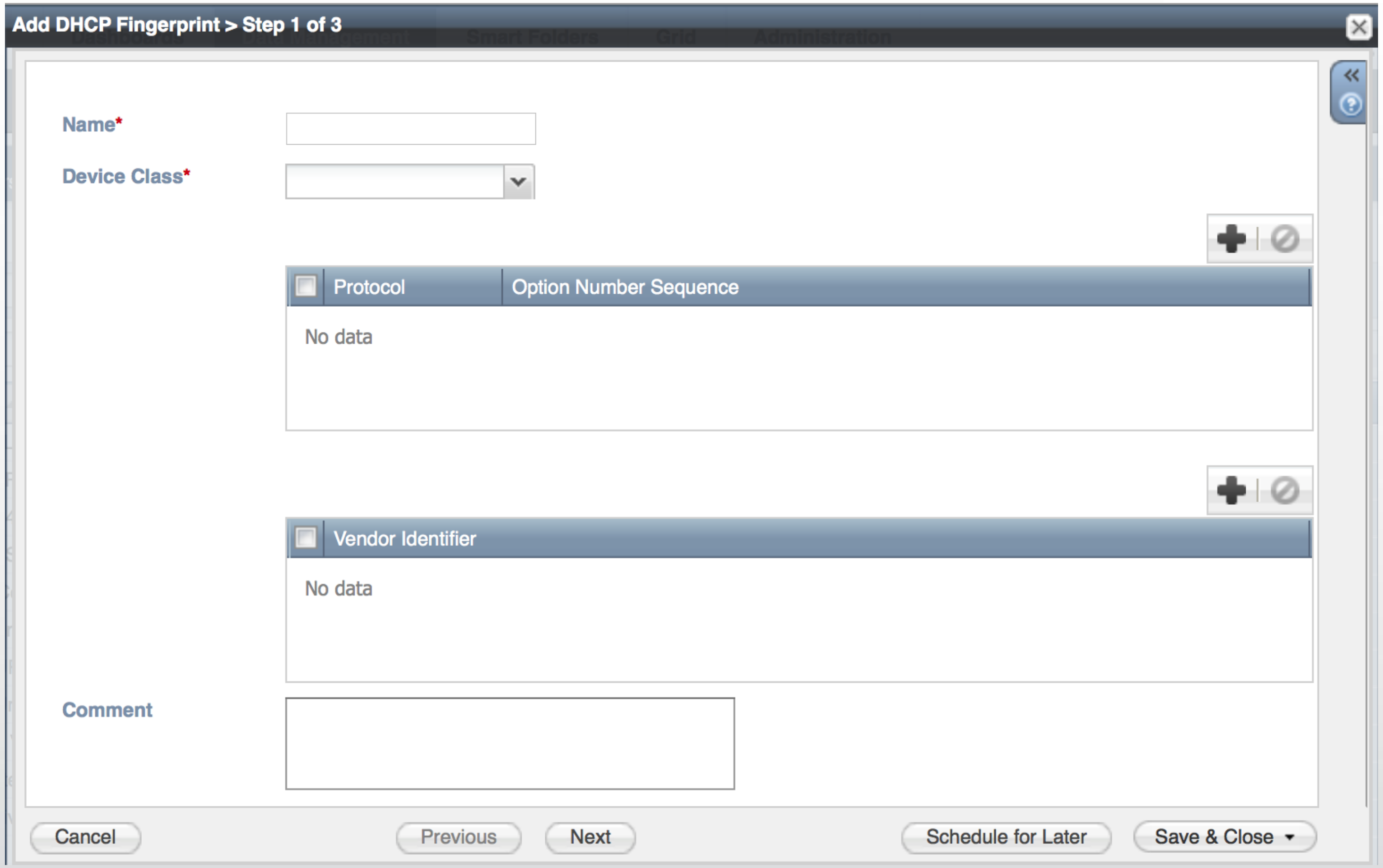
Use case – University Campus

- Separate handheld traffic from laptops on university wireless.
  - Filter handheld devices to specific Ranges of IP’s
  - Give preferential bandwidth to laptops
  - Block gaming devices from Campus Wireless

DHCP Fingerprinting

Creating custom fingerprints

- Add your own
- Simplified interface



Add DHCP Fingerprint > Step 1 of 3

Name*

Device Class*

□	Protocol	Option Number Sequence
No data		

□	Vendor Identifier
No data	

Comment

Insert Transition Slide – Lease History

Lease History

Lease-history

Issue

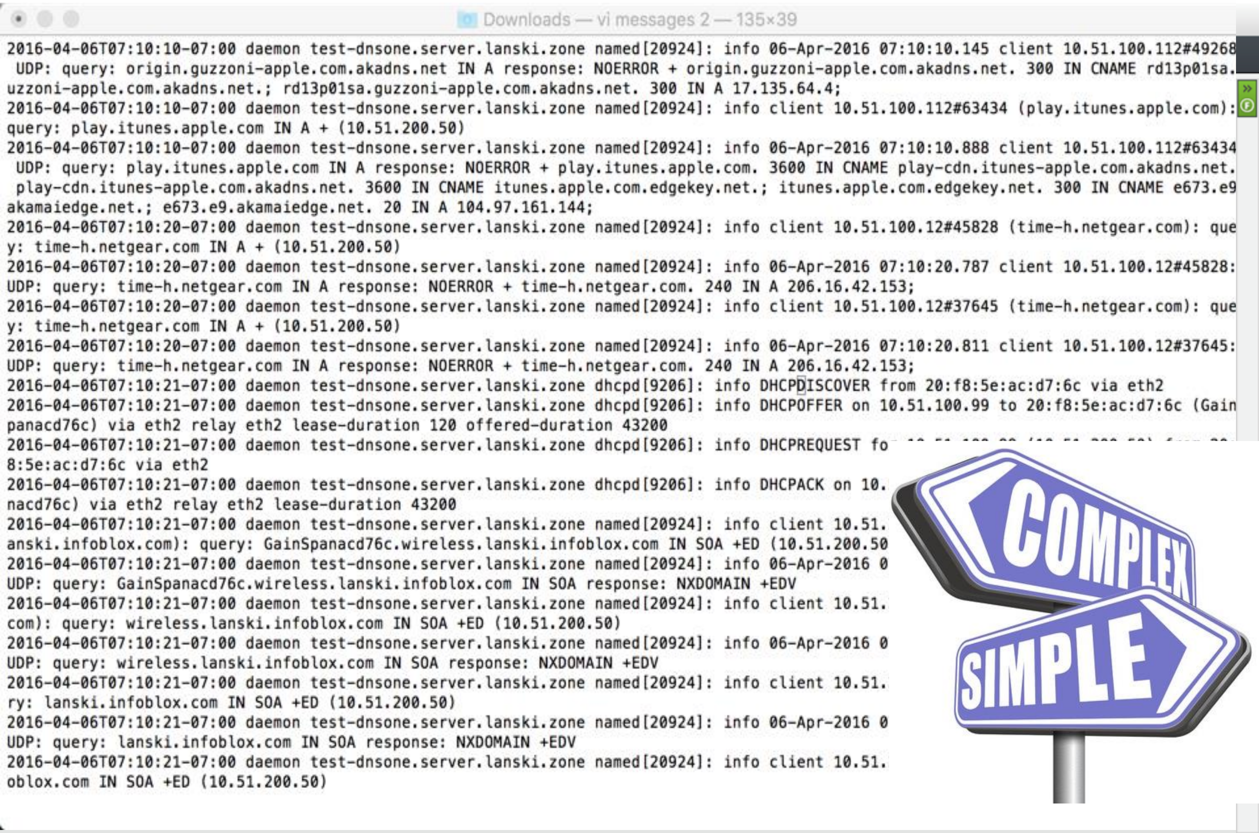
Lease-history

Use case – network configuration changed

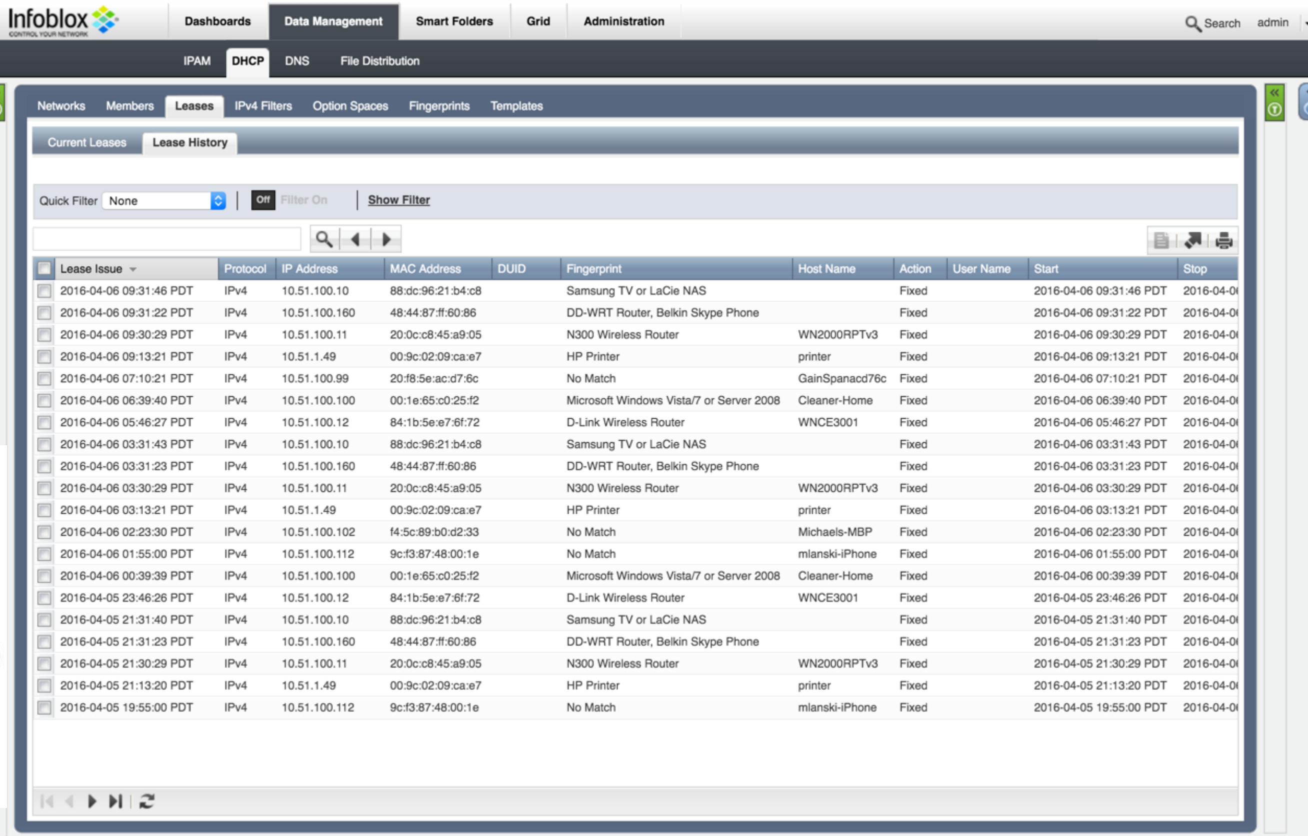
Who get’s in trouble?

Lease-history

How it works



```
2016-04-06T07:10:10-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info 06-Apr-2016 07:10:10.145 client 10.51.100.112#49268
 UDP: query: origin.guzzoni-apple.com.akadns.net IN A response: NOERROR + origin.guzzoni-apple.com.akadns.net. 300 IN CNAME rd13p01sa.
uzzoni-apple.com.akadns.net.; rd13p01sa.guzzoni-apple.com.akadns.net. 300 IN A 17.135.64.4;
2016-04-06T07:10:10-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info client 10.51.100.112#63434 (play.itunes.apple.com):
query: play.itunes.apple.com IN A + (10.51.200.50)
2016-04-06T07:10:10-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info 06-Apr-2016 07:10:10.888 client 10.51.100.112#63434
 UDP: query: play.itunes.apple.com IN A response: NOERROR + play.itunes.apple.com. 3600 IN CNAME play-cdn.itunes-apple.com.akadns.net.
 play-cdn.itunes-apple.com.akadns.net. 3600 IN CNAME itunes.apple.com.edgekey.net.; itunes.apple.com.edgekey.net. 300 IN CNAME e673.e9
akamaiedge.net.; e673.e9.akamaiedge.net. 20 IN A 104.97.161.144;
2016-04-06T07:10:20-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info client 10.51.100.12#45828 (time-h.netgear.com): que
y: time-h.netgear.com IN A + (10.51.200.50)
2016-04-06T07:10:20-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info 06-Apr-2016 07:10:20.787 client 10.51.100.12#45828:
UDP: query: time-h.netgear.com IN A response: NOERROR + time-h.netgear.com. 240 IN A 206.16.42.153;
2016-04-06T07:10:20-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info client 10.51.100.12#37645 (time-h.netgear.com): que
y: time-h.netgear.com IN A + (10.51.200.50)
2016-04-06T07:10:20-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info 06-Apr-2016 07:10:20.811 client 10.51.100.12#37645:
UDP: query: time-h.netgear.com IN A response: NOERROR + time-h.netgear.com. 240 IN A 206.16.42.153;
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone dhcpd[9206]: info DHCPDISCOVER from 20:f8:5e:ac:d7:6c via eth2
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone dhcpd[9206]: info DHCPOFFER on 10.51.100.99 to 20:f8:5e:ac:d7:6c (Gain
panacd76c) via eth2 relay eth2 lease-duration 120 offered-duration 43200
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone dhcpd[9206]: info DHCPREQUEST fo
8:5e:ac:d7:6c via eth2
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone dhcpd[9206]: info DHCPACK on 10.
nacd76c) via eth2 relay eth2 lease-duration 43200
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info client 10.51.
anski.infoblox.com): query: GainSpanacd76c.wireless.lanski.infoblox.com IN SOA +ED (10.51.200.50
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info 06-Apr-2016 0
UDP: query: GainSpanacd76c.wireless.lanski.infoblox.com IN SOA response: NXDOMAIN +EDV
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info client 10.51.
com): query: wireless.lanski.infoblox.com IN SOA +ED (10.51.200.50)
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info 06-Apr-2016 0
UDP: query: wireless.lanski.infoblox.com IN SOA response: NXDOMAIN +EDV
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info client 10.51.
ry: lanski.infoblox.com IN SOA +ED (10.51.200.50)
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info 06-Apr-2016 0
UDP: query: lanski.infoblox.com IN SOA response: NXDOMAIN +EDV
2016-04-06T07:10:21-07:00 daemon test-dnsone.server.lanski.zone named[20924]: info client 10.51.
oblox.com IN SOA +ED (10.51.200.50)
```



Quick Filter: None

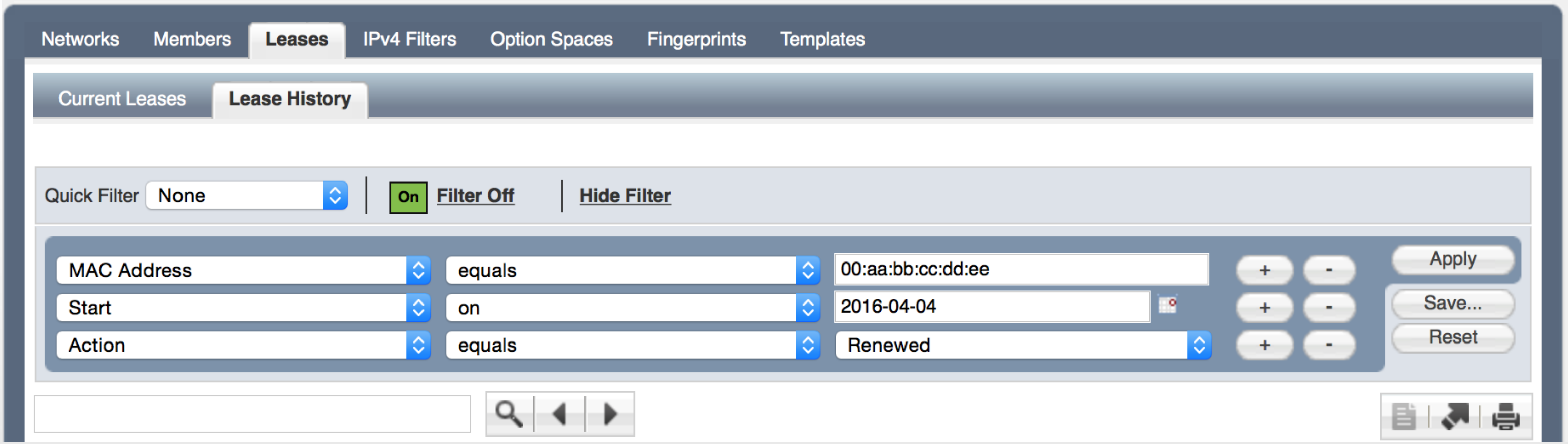
□	Lease Issue	Protocol	IP Address	MAC Address	DUID	Fingerprint	Host Name	Action	User Name	Start	Stop
□	2016-04-06 09:31:46 PDT	IPv4	10.51.100.10	88:dc:96:21:b4:c8		Samsung TV or LaCie NAS		Fixed		2016-04-06 09:31:46 PDT	2016-04-0
□	2016-04-06 09:31:22 PDT	IPv4	10.51.100.160	48:44:87:ff:60:86		DD-WRT Router, Belkin Skype Phone		Fixed		2016-04-06 09:31:22 PDT	2016-04-0
□	2016-04-06 09:30:29 PDT	IPv4	10.51.100.11	20:0c:c8:45:a9:05		N300 Wireless Router	WN2000RPTv3	Fixed		2016-04-06 09:30:29 PDT	2016-04-0
□	2016-04-06 09:13:21 PDT	IPv4	10.51.1.49	00:9c:02:09:ca:e7		HP Printer	printer	Fixed		2016-04-06 09:13:21 PDT	2016-04-0
□	2016-04-06 07:10:21 PDT	IPv4	10.51.100.99	20:f8:5e:ac:d7:6c		No Match	GainSpanacd76c	Fixed		2016-04-06 07:10:21 PDT	2016-04-0
□	2016-04-06 06:39:40 PDT	IPv4	10.51.100.100	00:1e:65:c0:25:f2		Microsoft Windows Vista/7 or Server 2008	Cleaner-Home	Fixed		2016-04-06 06:39:40 PDT	2016-04-0
□	2016-04-06 05:46:27 PDT	IPv4	10.51.100.12	84:1b:5e:e7:6f:72		D-Link Wireless Router	WNCE3001	Fixed		2016-04-06 05:46:27 PDT	2016-04-0
□	2016-04-06 03:31:43 PDT	IPv4	10.51.100.10	88:dc:96:21:b4:c8		Samsung TV or LaCie NAS		Fixed		2016-04-06 03:31:43 PDT	2016-04-0
□	2016-04-06 03:31:23 PDT	IPv4	10.51.100.160	48:44:87:ff:60:86		DD-WRT Router, Belkin Skype Phone		Fixed		2016-04-06 03:31:23 PDT	2016-04-0
□	2016-04-06 03:30:29 PDT	IPv4	10.51.100.11	20:0c:c8:45:a9:05		N300 Wireless Router	WN2000RPTv3	Fixed		2016-04-06 03:30:29 PDT	2016-04-0
□	2016-04-06 03:13:21 PDT	IPv4	10.51.1.49	00:9c:02:09:ca:e7		HP Printer	printer	Fixed		2016-04-06 03:13:21 PDT	2016-04-0
□	2016-04-06 02:23:30 PDT	IPv4	10.51.100.102	f4:5c:89:b0:d2:33		No Match	Michaels-MBP	Fixed		2016-04-06 02:23:30 PDT	2016-04-0
□	2016-04-06 01:55:00 PDT	IPv4	10.51.100.112	9c:f3:87:48:00:1e		No Match	mlanski-iPhone	Fixed		2016-04-06 01:55:00 PDT	2016-04-0
□	2016-04-06 00:39:39 PDT	IPv4	10.51.100.100	00:1e:65:c0:25:f2		Microsoft Windows Vista/7 or Server 2008	Cleaner-Home	Fixed		2016-04-06 00:39:39 PDT	2016-04-0
□	2016-04-05 23:46:26 PDT	IPv4	10.51.100.12	84:1b:5e:e7:6f:72		D-Link Wireless Router	WNCE3001	Fixed		2016-04-05 23:46:26 PDT	2016-04-0
□	2016-04-05 21:31:40 PDT	IPv4	10.51.100.10	88:dc:96:21:b4:c8		Samsung TV or LaCie NAS		Fixed		2016-04-05 21:31:40 PDT	2016-04-0
□	2016-04-05 21:31:23 PDT	IPv4	10.51.100.160	48:44:87:ff:60:86		DD-WRT Router, Belkin Skype Phone		Fixed		2016-04-05 21:31:23 PDT	2016-04-0
□	2016-04-05 21:30:29 PDT	IPv4	10.51.100.11	20:0c:c8:45:a9:05		N300 Wireless Router	WN2000RPTv3	Fixed		2016-04-05 21:30:29 PDT	2016-04-0
□	2016-04-05 21:13:20 PDT	IPv4	10.51.1.49	00:9c:02:09:ca:e7		HP Printer	printer	Fixed		2016-04-05 21:13:20 PDT	2016-04-0
□	2016-04-05 19:55:00 PDT	IPv4	10.51.100.112	9c:f3:87:48:00:1e		No Match	mlanski-iPhone	Fixed		2016-04-05 19:55:00 PDT	2016-04-0

Lease-history

Use case – file sharing

Lease-history

Advanced search



Quick Filter: None

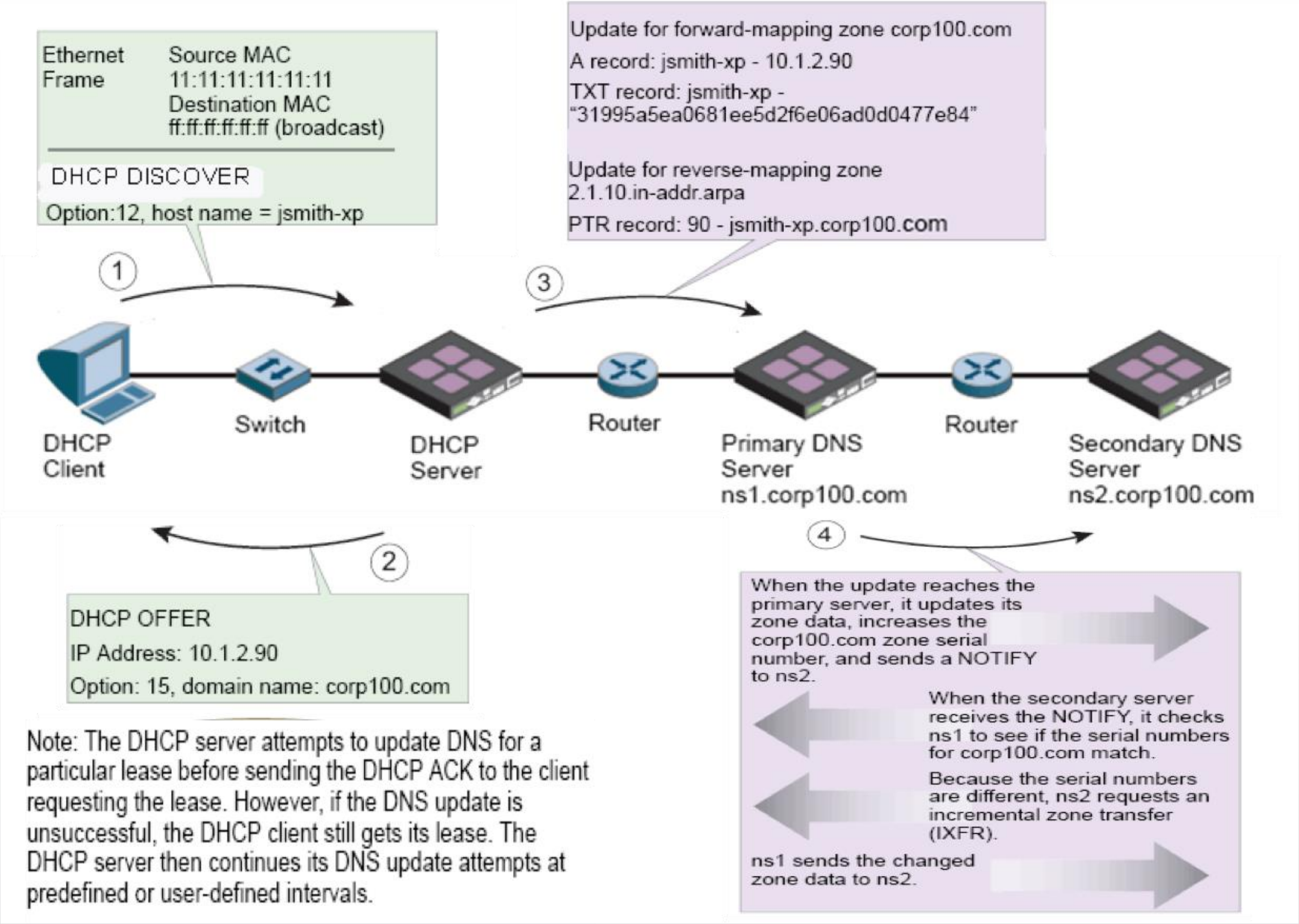
On Filter Off | Hide Filter

MAC Address	equals	00:aa:bb:cc:dd:ee
Start	on	2016-04-04
Action	equals	Renewed

DDNS

DDNS and DHCP Option-81

Overview of DDNS



1
2
3
4
DHCP Client
Switch
DHCP Server
Router
Primary DNS Server ns1.corp100.com
Router
Secondary DNS Server ns2.corp100.com

Ethernet Frame   Source MAC 11:11:11:11:11:11 Destination MAC ff:ff:ff:ff:ff:ff (broadcast)

DHCP DISCOVER

Option:12, host name = jsmith-xp

DHCP OFFER

IP Address: 10.1.2.90

Option: 15, domain name: corp100.com

Update for forward-mapping zone corp100.com

A record: jsmith-xp - 10.1.2.90

TXT record: jsmith-xp - "31995a5ea0681ee5d2f6e06ad0d0477e84"

Update for reverse-mapping zone 2.1.10.in-addr.arpa

PTR record: 90 - jsmith-xp.corp100.com

When the update reaches the primary server, it updates its zone data, increases the corp100.com zone serial number, and sends a NOTIFY to ns2.

When the secondary server receives the NOTIFY, it checks ns1 to see if the serial numbers for corp100.com match.

Because the serial numbers are different, ns2 requests an incremental zone transfer (IXFR).

ns1 sends the changed zone data to ns2.

Note: The DHCP server attempts to update DNS for a particular lease before sending the DHCP ACK to the client requesting the lease. However, if the DNS update is unsuccessful, the DHCP client still gets its lease. The DHCP server then continues its DNS update attempts at predefined or user-defined intervals.

DDNS

Understanding DDNS Security Options

- ISC
- Check-only
- ISC-Transitional
- No check

DDNS and DHCP Option-81

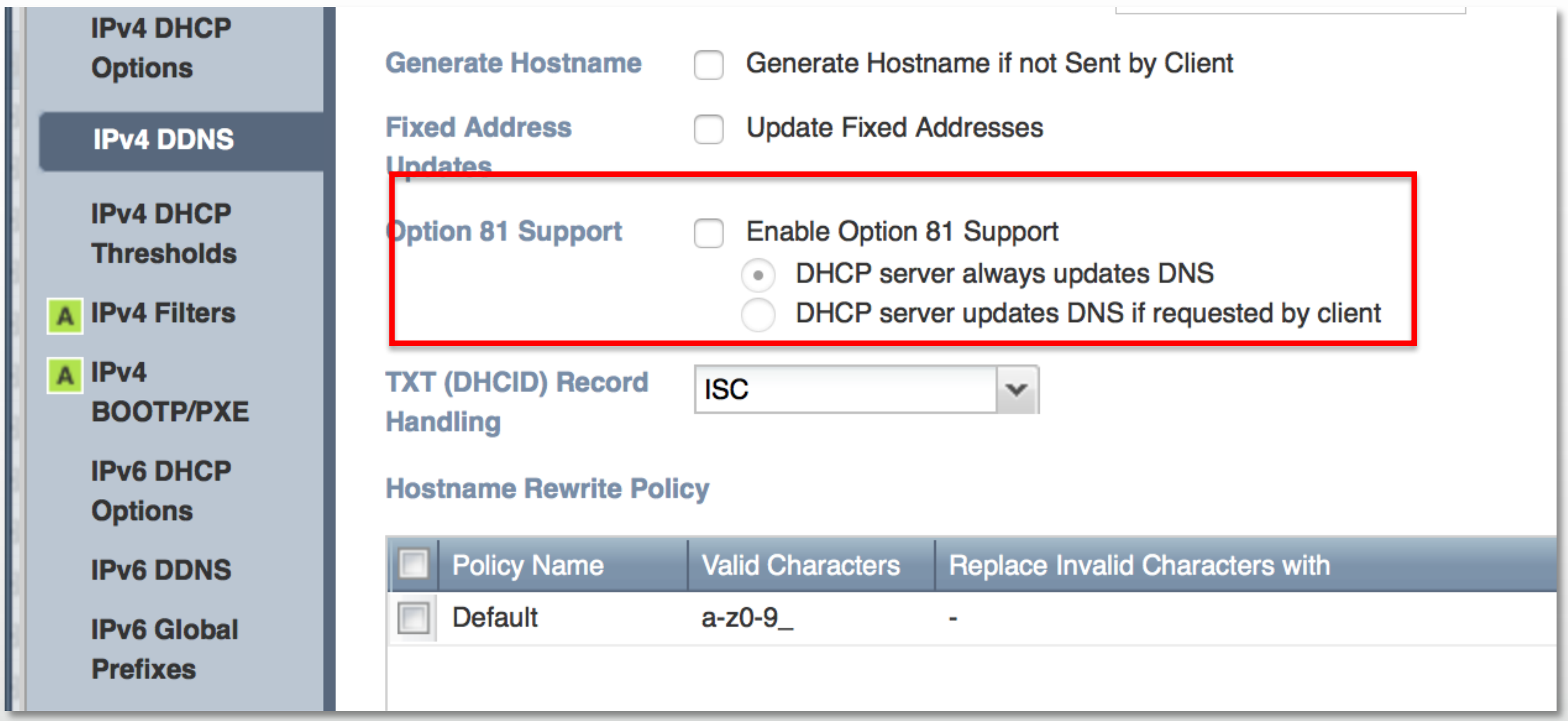
Overview of Option-81

DDNS and DHCP Option-81

Option-81 – Use Case

DDNS and DHCP Option-81

Server and client configuration



Generate Hostname ☐ Generate Hostname if not Sent by Client

Fixed Address Updates ☐ Update Fixed Addresses

Option 81 Support ☐ Enable Option 81 Support

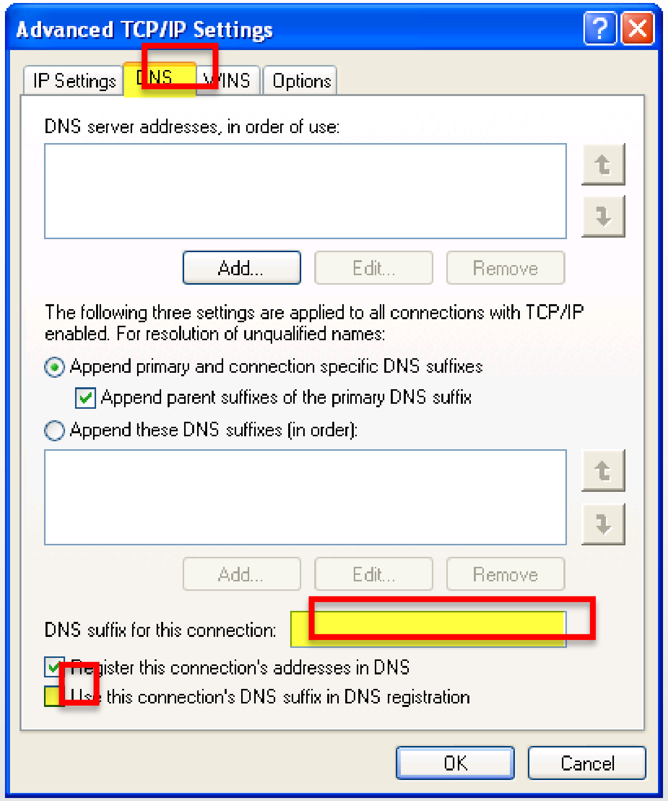
● DHCP server always updates DNS

○ DHCP server updates DNS if requested by client

TXT (DHCID) Record Handling: ISC

Hostname Rewrite Policy

☐	Policy Name	Valid Characters	Replace Invalid Characters with
☐	Default	a-z0-9_	-



DNS server addresses, in order of use:

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

DNS suffix for this connection:

☑ Register this connection's addresses in DNS

☐ Use this connection's DNS suffix in DNS registration

Questions?