Integrating L2/L3 Diagnostics : Nalini Elkins

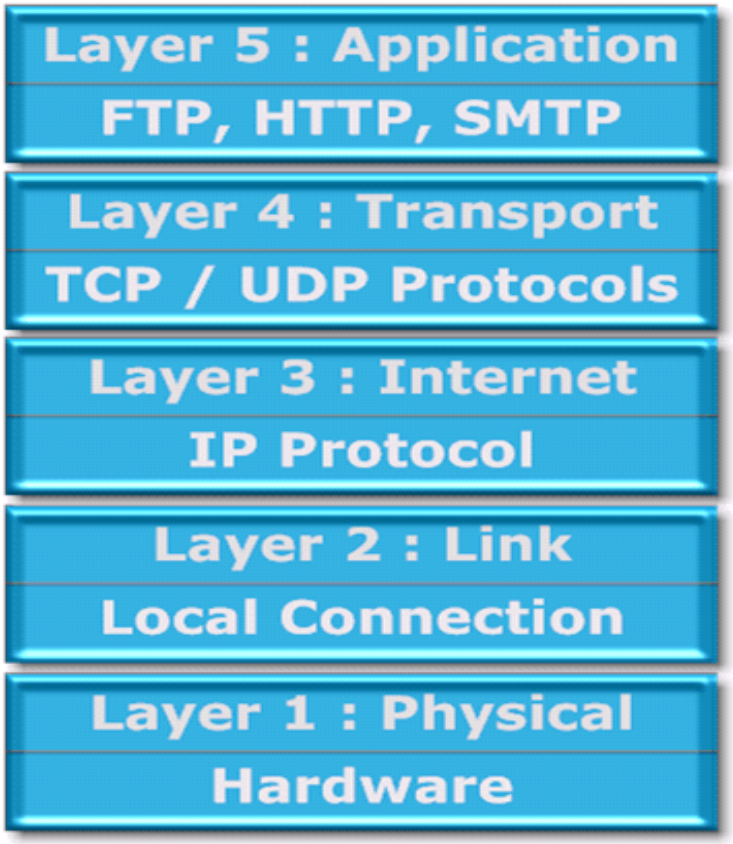
TCP/IP Layer Structure

TCP/IP layer structure.

Devices connect at different levels

Separation of function

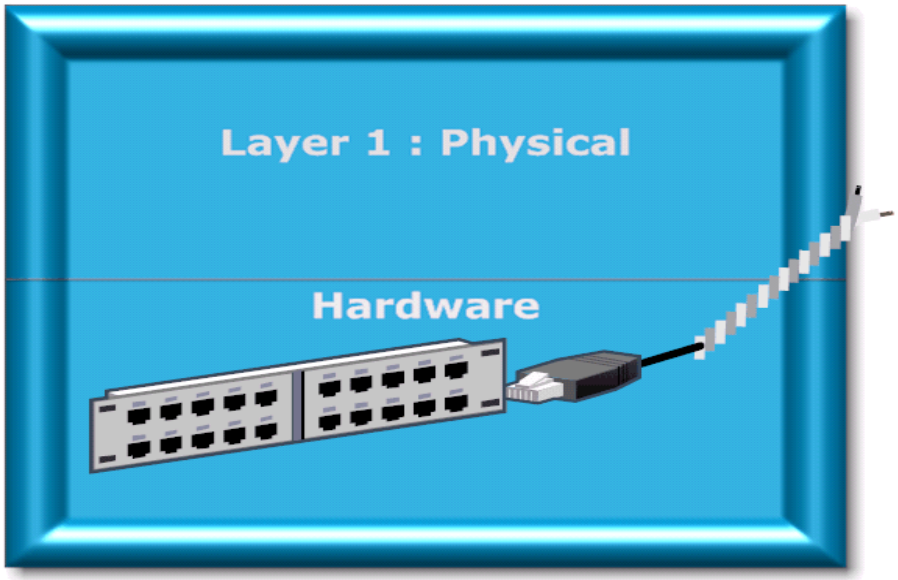
Each layer has its job to do



TCP/IP Layer 1

Physical or electrical connection

Cable from network to physical device



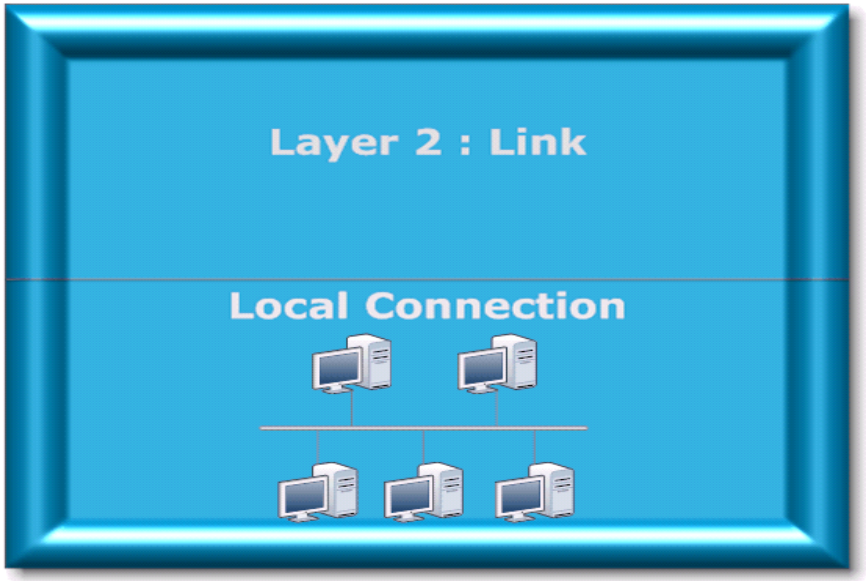
TCP/IP Layer 2

Data Link Layer

Logical connection between devices on same link

Same local area network or direct connection.

Anything where you don't go over a router

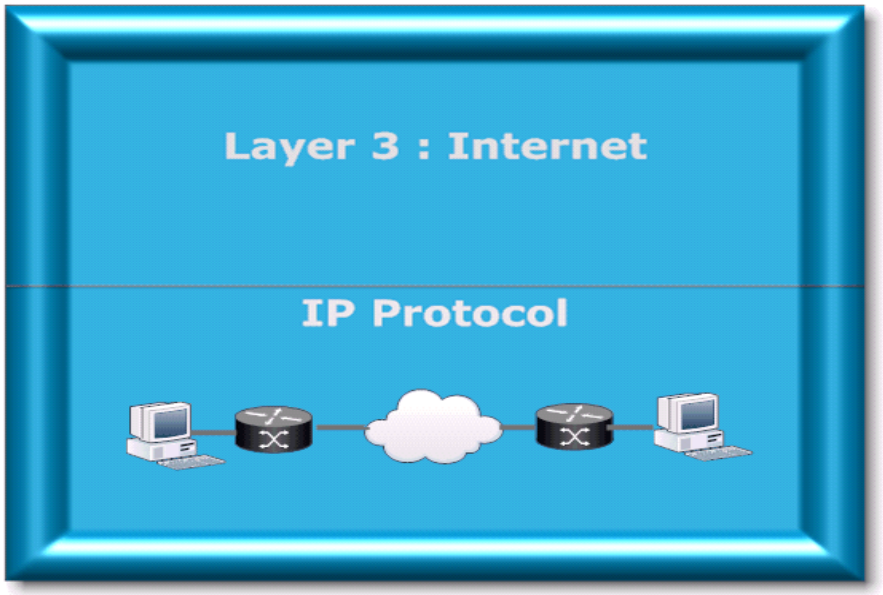


TCP/IP Layer 3

Logical connection between devices on network

Devices may be all over the world!

Routers in the Internet or Intranet



Layer 2 : Address Resolution

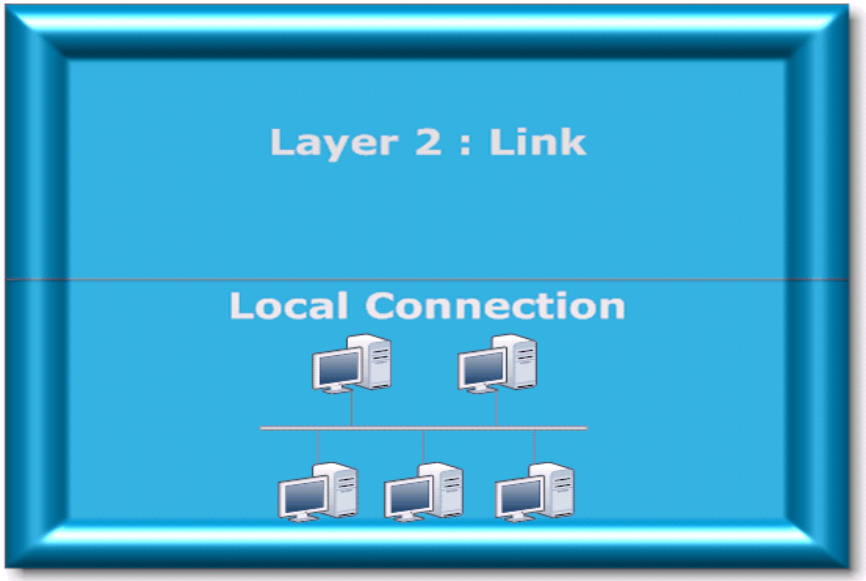
Data Link Layer

How is this done?

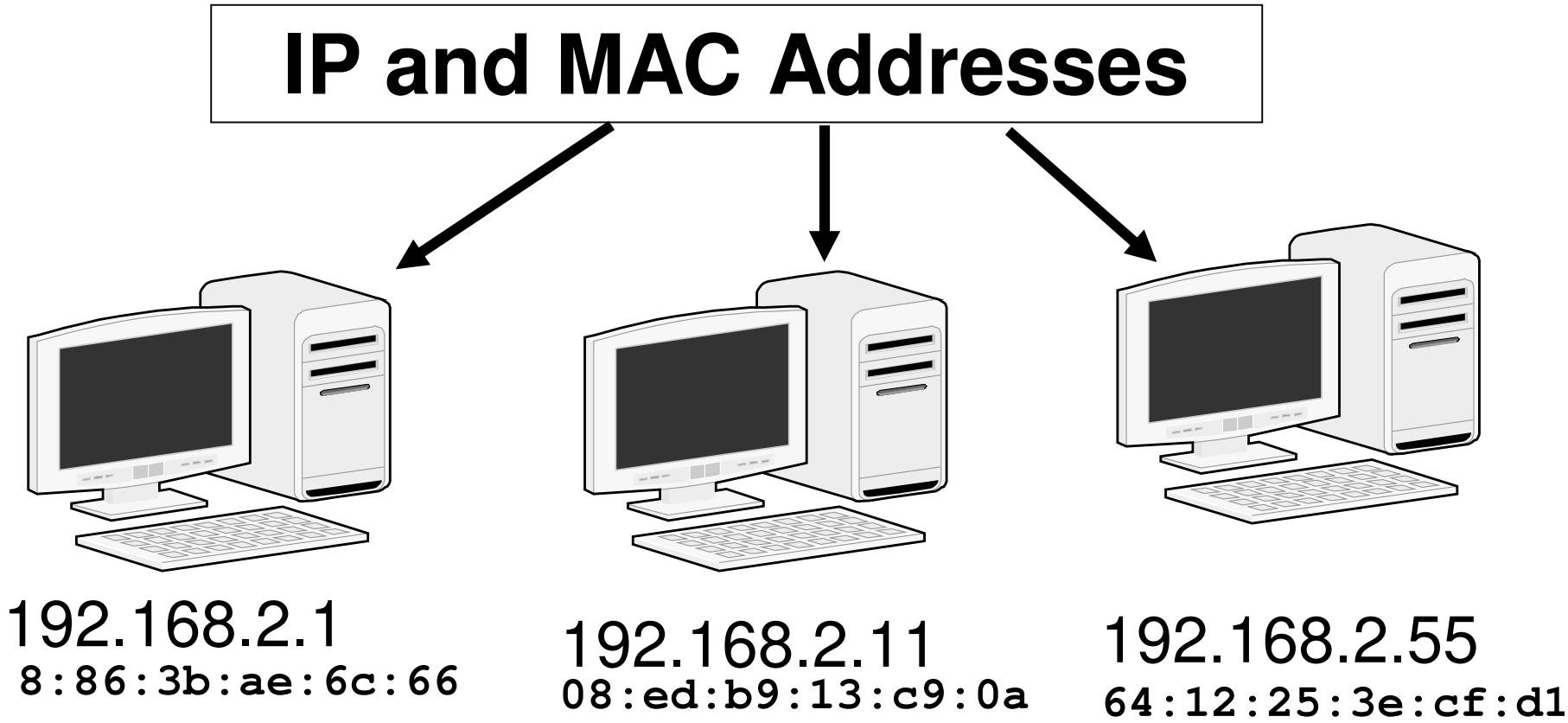
MAC addresses

IPv4: Address Resolution Protocol (between 2 and 3)

IPv6: Neighbor Discovery



Network Addresses



```
C:\Windows\system32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : nalinijoshi-HP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Belkin

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Virtual WiFi Miniport Adapter
   Physical Address. . . . . . . . . : 08-ED-B9-13-C9-0A
   DHCP Enabled. . . . . . . . . . . : Yes
```

```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : Belkin
   Description . . . . . . . . . . . : Broadcom 4313GN 802.11b/g/n 1x1 Wi-Fi Adapter
   Physical Address. . . . . . . . . : 08-ED-B9-13-C9-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a03b:4227:bf30:a085%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, September 23, 2014 4:50:47 AM
   Lease Expires . . . . . . . . . . : Friday, October 30, 2150 11:55:53 AM
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 319352249
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-16-77-75-01-A0-B3-CC-6B-AA-60

   DNS Servers . . . . . . . . . . . : 192.168.2.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : A0-B3-CC-6B-AA-60
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:6abd:38ca:2956:e77d:b50
```

MAC Addresses

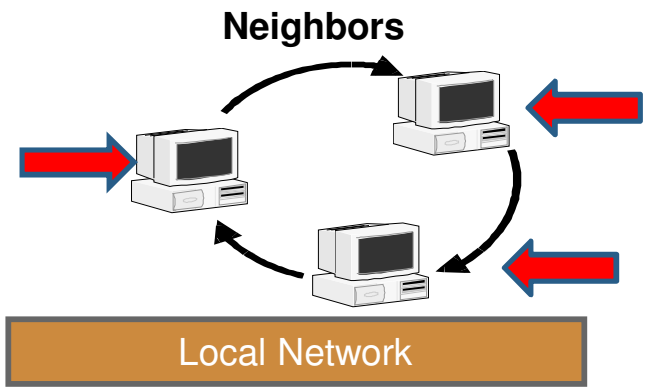
- Interface cards

1. Wireless
2. Ethernet
3. Virtual

- Made by a vendor

- Have a structured format

- IEEE regulates (Institute of Electrical and Electronics Engineers)



MAC Address Format

08-ED-B9-13-C9-0A

08-ED-B9 = OUI (MA-L)

13-C9-0A = NIC

- IEEE assigns first part
- Vendor assigns second part

IEEE New Naming Convention

- Introducing more user-friendly product names

- IEEE Registration Authority is implementing a more user-friendly naming convention for its products. In an effort to provide relevant and easy to identify names, we've incorporated the recognized term MAC (Media Access Control), along with the specific address "block" size (Large, Medium, Small), for those products that provide customers with MAC addresses:

- MAC Addresses - Large (MA-L) = 16 million 48-bit addresses—previously called OUI (OUI-24)

- MAC Addresses - Small (MA-S) = 4096 48-bit addresses—previously called OUI-36, but also encompassing IAB

IEEE OUI (MA-x) Public Information

Interface:d0:e1:40:96:71:10
Apple, Inc

```
D0-E1-40    (hex)          Apple, Inc
D0E140      (base 16)      Apple, Inc
                           1 infinite Loop
                           Cupertino CA 95014
                           UNITED STATES
```

Show Neighbors

```
C:\Windows\system32>netsh int ipv4 show nei

Interface 13: Wireless Network Connection


Internet Address                                      Physical Address   Type
----------------------------------------------------  -----------------  -----------
192.168.2.1                                           08-86-3b-ae-6c-66  Reachable
192.168.2.255                                         ff-ff-ff-ff-ff-ff  Permanent
224.0.0.2                                             01-00-5e-00-00-02  Permanent
224.0.0.22                                            01-00-5e-00-00-16  Permanent
224.0.0.252                                           01-00-5e-00-00-fc  Permanent
224.0.0.253                                           01-00-5e-00-00-fd  Permanent
239.255.255.250                                       01-00-5e-7f-ff-fa  Permanent
```

Special L2 / L3 Addresses

01:00:5E : IPv4 Multicast Interface Address

192.168.2.255 : Broadcast (ff-ff-ff-ff-ff-ff)

224.0.0.2 : All Routers on the same network segment (01-00-5e-00-00-02)

224.0.0.22 : Internet Group Management Protocol (IGMP)(01-00-5e-00-00-16)

224.0.0.252 : Link-local Mcast Name Resolution (LLMNR)(01-00-5e-00-00-fc)

224.0.0.253 : Teredo tunneling client discovery (01-00-5e-00-00-fd)

239.255.255.250 : Simple Service Discovery Protocol (01-00-5e-7f-ff-fa)

255.255.255.255 : Broadcast (ff-ff-ff-ff-ff-ff)

IPv4 multicast addresses: Class D: 224.0.0.0/4. Range from 224.0.0.0 - 239.255.255.255. 224.0.0.0 - 224.0.0.255 reserved for local subnet multicast traffic.

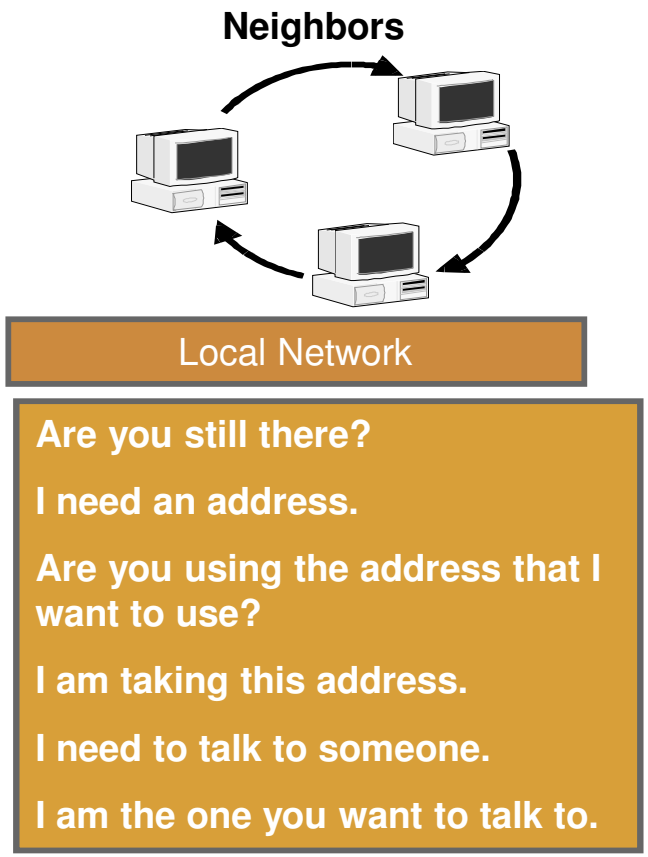
Let’s Look at a Packet

```
⊞ Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊟ Ethernet II, Src: BelkinIn_ae:6c:66 (08:86:3b:ae:6c:66), Dst: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a)
  ⊟ Destination: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a)
    Address: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: BelkinIn_ae:6c:66 (08:86:3b:ae:6c:66)
    Address: BelkinIn_ae:6c:66 (08:86:3b:ae:6c:66)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.2.1 (192.168.2.1), Dst: 192.168.2.11 (192.168.2.11)
```

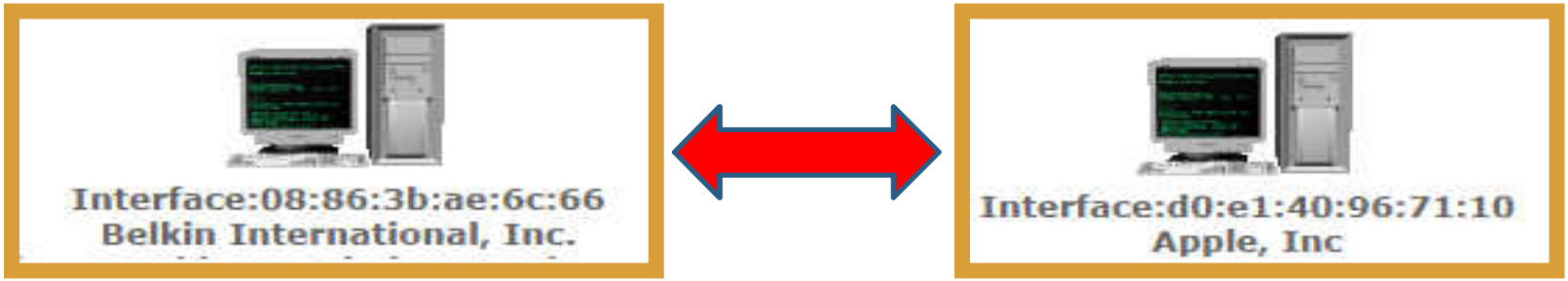
- On LAN
- Unicast traffic
- From 192.168.2.1 to 192.168.2.11
- Using unicast layer 2 addresses

Address Resolution Protocol

- How neighbors talk.
- What is a neighbor?
- What do they say?



How Neighbors Talk



- Use MAC addresses
- On local network

Portion of ARP Packet

```
Ethernet II,
Destination: 08:86:3b:ae:6c:66 (08:86:3b:ae:6c:66)
Source: 08:ed:b9:13:c9:0a (08:ed:b9:13:c9:0a)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 08:ed:b9:13:c9:0a (08:ed:b9:13:c9:0a)
    Sender IP address: 192.168.2.11 (192.168.2.11)
    Target MAC address: 08:86:3b:ae:6c:66 (08:86:3b:ae:6c:66)
```

Let’s Look at another Packet

```
⊞ Frame 4: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
⊟ Ethernet II, Src: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a), Dst: BelkinIn_ae:6c:66 (08:86:3b:ae:6c:66)
  ⊟ Destination: BelkinIn_ae:6c:66 (08:86:3b:ae:6c:66)
      Address: BelkinIn_ae:6c:66 (08:86:3b:ae:6c:66)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ⊟ Source: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a)
      Address: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.2.11 (192.168.2.11), Dst: 74.125.224.78 (74.125.224.78)
```

- Unicast traffic
- From 192.168.2.11 to 74.125.224.78
- Using unicast layer 2 addresses
- But whose?
- I thought Router IP address was 192.168.1.1

From ARIN Address Lookup

Network	
NetRange	74.125.0.0 - 74.125.255.255
CIDR	74.125.0.0/16
Name	GOOGLE
Handle	NET-74-125-0-0-1
Parent	NET74 (NET-74-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Google Inc. (GOGL)
Registration Date	2007-03-13
Last Updated	2012-02-24

74.125.224.78 is Google!

If going outside…

- Router address given
- Router says “I am that device”
- Or coming in from the outside!

Router “Proxys”

Interface:08:86:3b:ae:6c:66
Belkin International, Inc.
The following IP Addresses belong to the same device :

192.168.2.1	This is an IPv4 Private Address		Packets sent TO and FROM address	
FE80::8000:F227:A10A:8602	This is an IPv6 Link-Local Address		Packets sent FROM address	
23.210.251.120	a23-210-251-120.deploy.static	akamaitechnologies.com	This is an IPv4 Public Address	
65.54.167.8			This is an IPv4 Public Address	
68.142.253.31	UNKNOWN-68-142-253-X	yahoo.com	This is an IPv4 Public Address	
74.125.28.84	pc-in-f84	1e100.net (Google)	This is an IPv4 Public Address	
74.125.28.125			This is an IPv4 Public Address	
74.125.28.188	pc-in-f188	1e100.net (Google)	This is an IPv4 Public Address	
74.125.224.78	lax17s02-in-f14	1e100.net (Google)	This is an IPv4 Public Address	
74.125.239.97	nuq05s01-in-f1	1e100.net (Google)	This is an IPv4 Public Address	
74.125.239.99	nuq05s01-in-f3	1e100.net (Google)	This is an IPv4 Public Address	
98.136.189.19	pr.comet.vip.gq1	yahoo.com	This is an IPv4 Public Address	
98.136.223.38	pprd1-rtr1.manhattan.vip.gq1	yahoo.com	This is an IPv4 Public Address	
98.138.81.72	r1.ycpi.vip.ne1	yahoo.net	This is an IPv4 Public Address	
98.138.243.53	yts2.yql.vip.ne1	yahoo.com	This is an IPv4 Public Address	
98.138.253.63	pprd1-rtr1.manhattan.vip.ne1	yahoo.com	This is an IPv4 Public Address	
206.190.61.106	r1.ycpi.vip.sjb	yahoo.net	This is an IPv4 Public Address	
206.190.61.107		yahoo.net	This is an IPv4 Public Address	

All addresses have router MAC address

Packet Inside Network

```
Ethernet II,
Destination: 08:86:3b:ae:6c:66 (08:86:3b:ae:6c:66)
Source: 08:ed:b9:13:c9:0a (08:ed:b9:13:c9:0a)


Internet Protocol Version 4,
Src: 192.168.2.11 (192.168.2.11),
Dst: 192.168.2.1 (192.168.2.1)
```

Same subnet

Interface:08:86:3b:ae:6c:66
Belkin International, Inc.

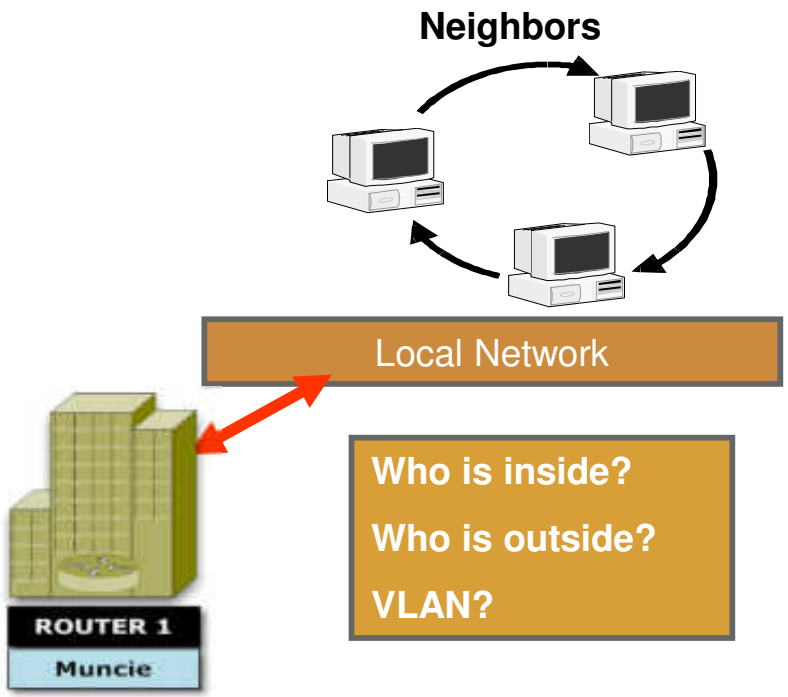
Packet Outside Network

```
Ethernet II,
Src: 08:ed:b9:13:c9:0a (08:ed:b9:13:c9:0a),
Dst: 08:86:3b:ae:6c:66 (08:86:3b:ae:6c:66)

Internet Protocol Version 4,
Src: 192.168.2.11 (192.168.2.11),
Dst: 23.210.251.120 (23.210.251.120)
```

Different subnets

Deduce Network Configuration

- Look at Layer 2 and match with Layer 3
- Who is inside / who is outside
- VLANs (multiple subnets)
- Public addresses for internal network
- Depends on where trace is done



Diagnostics

Device

Interface:08:86:3b:ae:6c:66
Belkin International, Inc.
The following IP Addresses are the router private addresses or addresses on a VLAN:

192.168.2.1	Home Router	Home LAN	This is an IPv4 Private Address	Packets sent TO and FROM address
FE80::8000:F227:62C7:9542			This is an IPv6 Link-Local Address	Packets sent FROM address

The following IP Addresses are coming from outside this network:

64.4.23.142	Hotmail	Microsoft.com	This is an IPv4 Public Address	Packets sent TO and FROM address
64.4.23.147	Hotmail	Microsoft.com	This is an IPv4 Public Address	Packets sent TO and FROM address
64.4.23.160	Hotmail	Microsoft.com	This is an IPv4 Public Address	Packets sent TO and FROM address
64.4.23.162	Hotmail	Microsoft.com	This is an IPv4 Public Address	Packets sent TO and FROM address
64.4.23.165	Hotmail	Microsoft.com	This is an IPv4 Public Address	Packets sent TO and FROM address
64.4.23.174	Hotmail	Microsoft.com	This is an IPv4 Public Address	Packets sent TO and FROM address
64.4.23.176	Hotmail	Microsoft.com	This is an IPv4 Public Address	Packets sent TO and FROM address
74.125.21.138	yv-in-f138	1e100.net (Google)	This is an IPv4 Public Address	Packets sent TO and FROM address

- I have a slow down on my home network
- Who is the router?

Who else is on my network?

2

Interface:00:1e:8f:93:7c:37
CANON INC.
The following IP Addresses belong to the same device :

192.168.2.8	Printer	Home LAN	This is an IPv4 Private Address	Packets sent FROM address

3

Interface:74:de:2b:ce:02:15
Liteon Technology Corporation
The following IP Addresses belong to the same device :

192.168.2.3	Unknown	Home LAN	This is an IPv4 Private Address	Packets sent TO and FROM address
FE80::FFFF:FFFF:FFFE			This is an IPv6 Teredo Link-Local Address	Packets sent TO and FROM address
FE80::3C28:26BA:3C3C:35F			This is an IPv6 Link-Local Address	Packets sent FROM address

224.0.0.251	Multicast DNS (mDNS)	This is an IPv4 Multicast Address	Packets sent TO address
239.255.255.250	Simple Service Discovery Protocol	This is an IPv4 Multicast Address	Packets sent TO address

4

Interface:78:6c:1c:b9:3f:7c
Apple
The following IP Addresses belong to the same device :

192.168.2.2	Home LAN	This is an IPv4 Private Address	Packets sent FROM address

Apple, Canon, Liteon interfaces

What are they doing?

-	-	Source Domain	Total Packets		Total Bytes		Average Segment Length
1		Home LAN	11K	(87.47%)	3M	(68.21%)	67
2		yahoo.net	799	(6.01%)	1M	(27.44%)	913
3		unresolved	331	(2.49%)	29K	(0.57%)	45
4		1e100.net (Google)	226	(1.7%)	64K	(1.23%)	185
5		yahoo.com	126	(0.94%)	91K	(1.76%)	494
6		windstream.net	85	(0.63%)	20K	(0.39%)	243
7		Microsoft.com	20	(0.15%)	470	(0.0%)	23
8		akamaitechnologies.com	17	(0.12%)	10K	(0.19%)	594
9		dropbox.com	16	(0.12%)	358	(0.0%)	22
10		expertcity.com	12	(0.09%)	0	(0.0%)	0
11		skype.com	11	(0.08%)	500	(0.0%)	33
12		secureserver.net	11	(0.08%)	6K	(0.13%)	621
13		live.com	7	(0.05%)	5	(0.0%)	0
14		hamachi.cc	2	(0.01%)	0	(0.0%)	0
15		inetia.pl	1	(0.0%)	0	(0.0%)	0
	Total		13K		5M		-

Lot of traffic from my home LAN

What addresses?

-	-	Source Address	Domain	Total Packets	Total Bytes	Average Segment Length
1		Printer 192.168.2.8	Home LAN	9K (71.06%)	3M (60.59%)	272
2		Unknown 192.168.2.3	Home LAN	1K (13.57%)	343K (6.63%)	63
3		r2.ycpi.vip.ac4 98.136.145.153	yahoo.net	703 (5.29%)	1M (24.55%)	1234
4		Home Router 192.168.2.1	Home LAN	367 (2.76%)	51K (0.98%)	78
5		yv-in-f138 74.125.21.138	1e100.net (Google)	117 (0.88%)	39K (0.76%)	337
6		l3.ycs.vip.sjb 206.190.60.139	yahoo.com	103 (0.77%)	84K (1.62%)	785
7		h64.228.189.173.dynamic.ip 173.189.228.64	windstream.net	85 (0.63%)	20K (0.39%)	243
8		yh-in-f125 74.125.137.125	1e100.net (Google)	78 (0.58%)	16K (0.32%)	130
9		r4.ycpi.vip.ac4 98.136.145.155	yahoo.net	74 (0.55%)	136K (2.63%)	568
10		213.199.179.160		40 (0.3%)	943 (0.01%)	23
	Total	-		13K	5M	-

What is my printer doing?

Lots of UDP Traffic!

-	-	Source Address	Domain	Total Packets	Total Bytes	Average Segment Length
1		Printer 192.168.2.8	Home LAN	9K (91.47%)	3M (96.56%)	272
2		Unknown 192.168.2.3	Home LAN	456 (4.41%)	37K (1.15%)	41
3		Home Router 192.168.2.1	Home LAN	247 (2.39%)	47K (1.46%)	171
4		h64.228.189.173.dynamic.ip 173.189.228.64	windstream.net	85 (0.82%)	20K (0.63%)	243
5		192.168.2.2		9 (0.08%)	3K (0.09%)	356
6		FE80::3C28:26BA:3C3C:35F		6 (0.05%)	180 (0.0%)	30
7		Nalini Phone 192.168.2.10	Home LAN	6 (0.05%)	264 (0.0%)	44
8		192.168.2.6		4 (0.03%)	424 (0.01%)	106
9		Hotmail 64.4.23.165	Microsoft.com	2 (0.01%)	40 (0.0%)	20
10		Hotmail 64.4.23.142	Microsoft.com	2 (0.01%)	52 (0.0%)	26

- I look at traffic by protocol
- What is my *#@& printer doing?

Looks Like DNS - Responses

Source Interface	Destination Interface	Source Address	Source Port	Destination Address	Total Packets	Total Bytes	DNS Error Code
00:1e:8f:93:7c:37	74:de:2b:ce:02:15	192.168.2.8	5353	224.0.0.251	9K	3M	0
dc:86:d8:9c:6f:e4	74:de:2b:ce:02:15	192.168.2.6	5353	224.0.0.251	4	424	0
78:6c:1c:b9:3f:7c	74:de:2b:ce:02:15	192.168.2.2	5353	224.0.0.251	6	2K	0
08:86:3b:ae:6c:66	74:de:2b:ce:02:15	192.168.2.1	53	192.168.2.3	18	2K	0

- Look by port
- Any queries?
- Notice destination is Multicast DNS (mDNS)

What are these?

-	-	Packet Number	Packet Date	Source Address	Source Port	Destination Address	Destination Port	Transaction ID	Flags	Resource	Query Type	Data Length
1		11	2014-03-11 08:55:44.340687	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
2		12	2014-03-11 08:55:44.341092	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340
3		13	2014-03-11 08:55:44.341306	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_http._tcp.local	A	249
4		18	2014-03-11 08:55:44.943990	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
5		19	2014-03-11 08:55:44.944194	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340
6		20	2014-03-11 08:55:44.944279	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_http._tcp.local	A	249
7		21	2014-03-11 08:55:44.944360	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
8		22	2014-03-11 08:55:44.944437	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340
9		25	2014-03-11 08:55:45.050933	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_http._tcp.local	A	249
10		26	2014-03-11 08:55:45.052695	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
11		27	2014-03-11 08:55:45.052965	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340

From RFC 6762 (MDNS)

- Typically a Multicast DNS responder should have, at the very least, address records for all of its active interfaces. Creating and advertising an HINFO record on each interface as well can be useful to network administrators.

- Whenever a Multicast DNS responder starts up, wakes up from sleep, receives an indication of a network interface "Link Change" event, or has any other reason to believe that its network connectivity may have changed in some relevant way, it MUST perform the two startup steps below: Probing and Announcing .

From RFC 6762

Flood protection

To protect the network against excessive packet flooding due to software bugs or malicious attack, a Multicast DNS responder MUST NOT (except in the one special case of answering probe queries) multicast a record on a given interface until at least one second has elapsed since the last time that record was multicast on that particular interface.

Let’s check the frequency

-	-	Packet Number	Packet Date	Source Address	Source Port	Destination Address	Destination Port	Transaction ID	Flags	Resource	Query Type	Data Length
1		11	2014-03-11 08:55:44.340687	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
2		12	2014-03-11 08:55:44.341092	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340
3		13	2014-03-11 08:55:44.341306	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_http._tcp.local	A	249
4		18	2014-03-11 08:55:44.943990	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
5		19	2014-03-11 08:55:44.944194	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340
6		20	2014-03-11 08:55:44.944279	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_http._tcp.local	A	249
7		21	2014-03-11 08:55:44.944360	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
8		22	2014-03-11 08:55:44.944437	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340
9		25	2014-03-11 08:55:45.050933	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_http._tcp.local	A	249
10		26	2014-03-11 08:55:45.052695	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_canon-bjnp1._tcp.local	A	408
11		27	2014-03-11 08:55:45.052965	192.168.2.8	5353	224.0.0.251	5353	0x0000	0x8400	_scanner._tcp.local	A	340

IPv4 Multicast Addresses

224.0.0.0= Base address (reserved)

224.0.0.1= All Hosts on same network segment

224.0.0.2= All Routers on the same network segment

224.0.0.4= Distance Vector Multicast Routing Protocol (DVMRP) to address multicast routers

224.0.0.5= Open Shortest Path First (OSPF) All OSPF Routers on network segment

224.0.0.6= OSPF All Designated Routers (DR) to designated routers on network segment

224.0.0.9= Routing Information Protocol (RIP) version2 on network segment

224.0.0.10= Enhanced Interior Gateway Routing Protocol (EIGRP) on network segment

224.0.0.13= Protocol Independent Multicast (PIM) Version2

224.0.0.18= Virtual Router Redundancy Protocol (VRRP)

224.0.0.19= IS-IS over IP

224.0.0.20= IS-IS over IP

224.0.0.21= IS-IS over IP

224.0.0.22= Internet Group Management Protocol (IGMP)

224.0.0.102= Hot Standby Router Protocol version2 (HSRPv2) / Gateway Load Balancing

224.0.0.107= Precision Time Protocol version2 peer delay measurement messaging

224.0.0.251= Multicast DNS (mDNS)

Resolution?

- Turned off printer!
- Could be power problem

More complications

- IPSec
- IPv6
- Anonymous proxy

Using IPSec

```
696 26.063989   15.168.1.24   15.168.1.23   ESP   ESP (SPI=0x0df7f301)

Frame 696: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
Ethernet II, Src: QuantaCo_b8:04:8c (04:7d:7b:b8:04:8c), Dst: Hewlett-_7a:78:86 (78:e3:b5:7a:78:86)
  Destination: Hewlett-_7a:78:86 (78:e3:b5:7a:78:86)
  Source: QuantaCo_b8:04:8c (04:7d:7b:b8:04:8c)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 15.168.1.24 (15.168.1.24), Dst: 15.168.1.23 (15.168.1.23)
Encapsulating Security Payload
  ESP SPI: 0x0df7f301 (234353409)
  ESP Sequence: 1
```

With IPSec (ESP), very little diagnostic information available

```
1222 108.916760   2601:648:8600:6a39:7ae3:b5ff:fe7a:7886   2601:648:8600:6a39:67d:7bff:feb8:48c

Frame 1222: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: Hewlett-_7a:78:86 (78:e3:b5:7a:78:86), Dst: QuantaCo_b8:04:8c (04:7d:7b:b8:04:8c)
  Destination: QuantaCo_b8:04:8c (04:7d:7b:b8:04:8c)
  Source: Hewlett-_7a:78:86 (78:e3:b5:7a:78:86)
  Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2601:648:8600:6a39:7ae3:b5ff:fe7a:7886 (2601:648:8600:6a39:7ae3:b5ff:
Encapsulating Security Payload
  ESP SPI: 0x089fd20c (144691724)
  ESP Sequence: 1
```

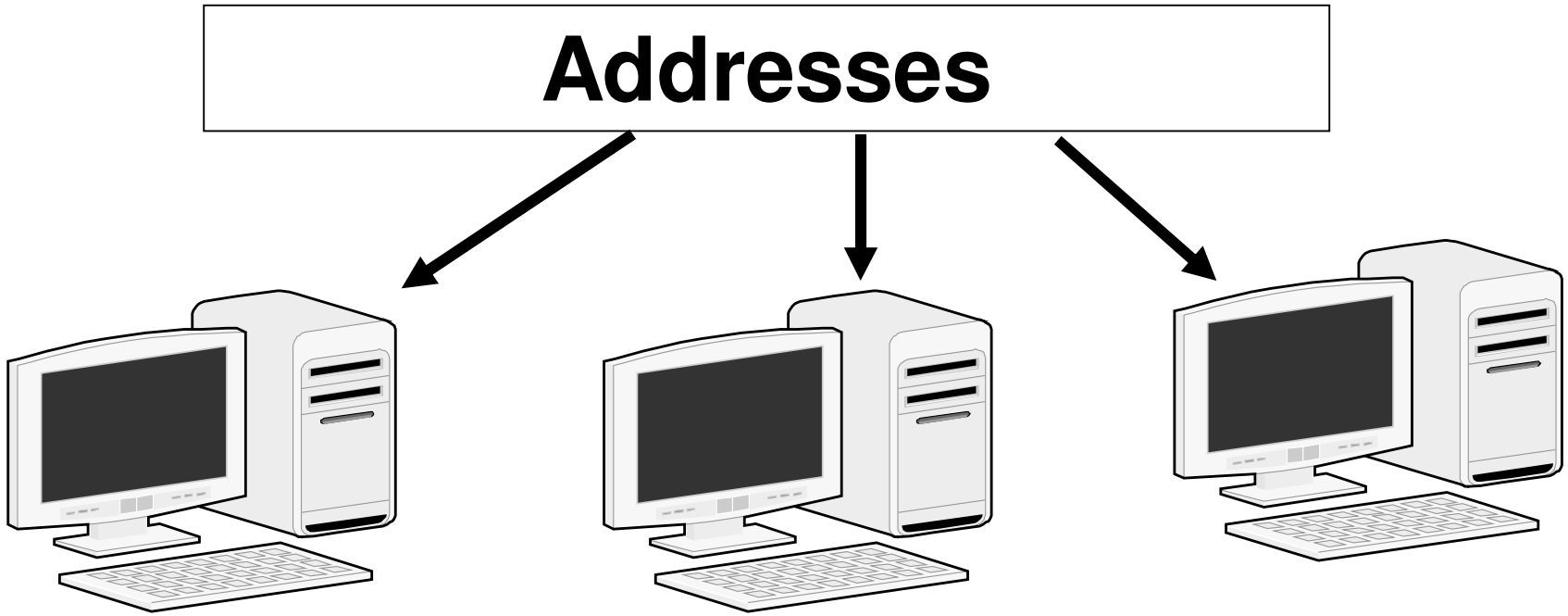
What about IPv6?

```
Windows IP Configuration:

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix  : hsd1.ca.comcast.net.
IPv6 Address. . . . . . . . . . : 2601:642:c200:da62:a03b:4227:bf30:a085
Temporary IPv6 Address. . . . . : 2601:642:c200:da62:d109:5962:7eed:9bc4
Link-local IPv6 Address . . . . : fe80::a03b:4227:bf30:a085%12
IPv4 Address. . . . . . . . . . : 10.0.0.3
Subnet Mask . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . : fe80::beca:b5ff:fedd:9de1%12
                                  10.0.0.1
```

What is physical address?

```
Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix: hsd1.ca.comcast.net.
Description . . . . . : Broadcom 4313GN 802.11b/g/n 1x1 Wi-Fi
Physical Address. . . . . : 08-ED-B9-13-C9-0A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . : Yes
IPv6 Address. . . . . : 2601:642:c200:da62:a03b:4227:bf30:a085(Preferred)
Temporary IPv6 Address: 2601:642:c200:da62:d109:5962:7eed:9bc4(Preferred)
Link-local IPv6 Address . . . : fe80::a03b:4227:bf30:a085%12(Preferred)
IPv4 Address. . . . . : 10.0.0.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::beca:b5ff:fedd:9de1%12
                                    10.0.0.1
```

TCP/IP Network

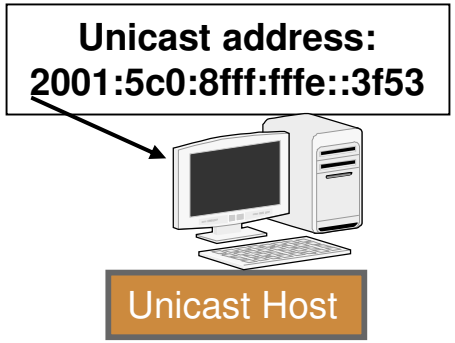


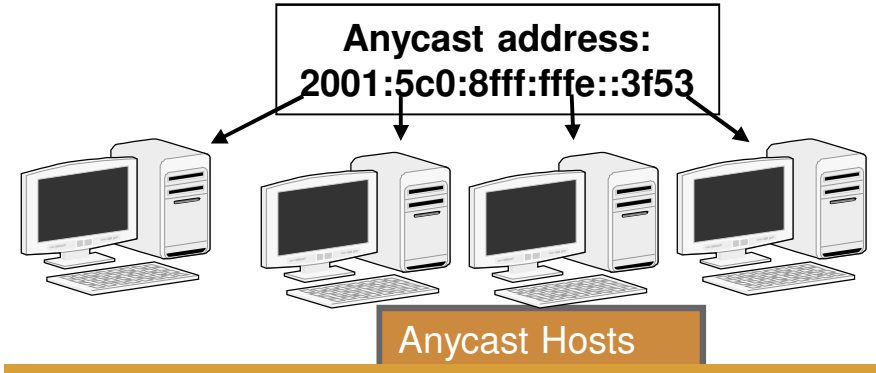
192.168.1.100
2001:5c0:8fff:3::100
fe80::1234:5678:abcd:1

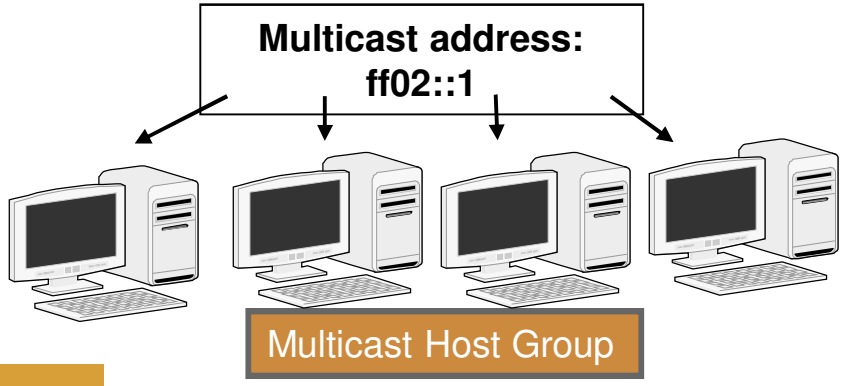
192.168.1.101
2001:5c0:8fff:3::101
fe80::1234:5678:ffff:3

192.168.1.102
2001:5c0:8fff:3::102
fe80::1234:5678:5555:6

IPv6 Address Types







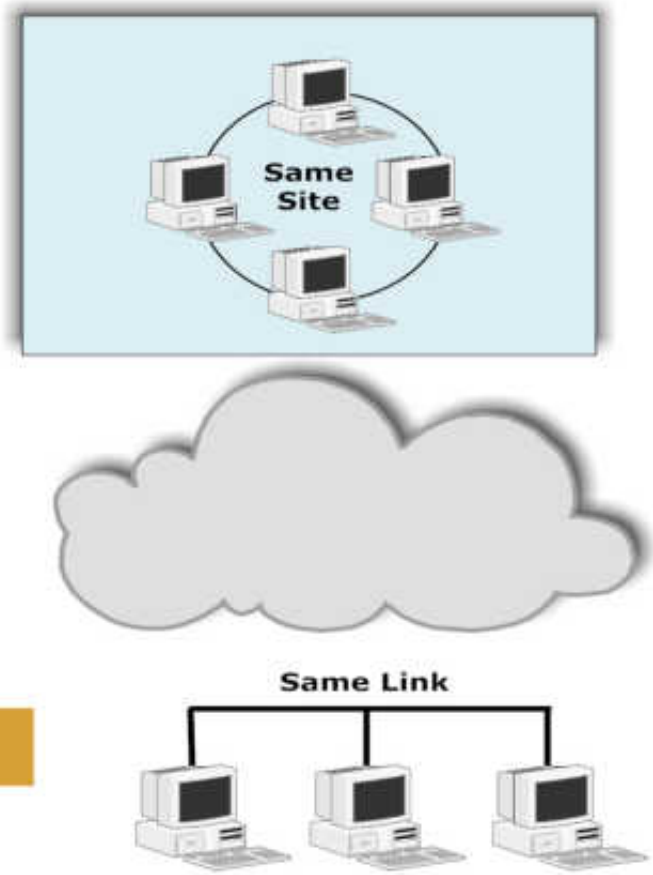
Anycast addresses appear the same as unicast addresses

IPv6 Private Addresses

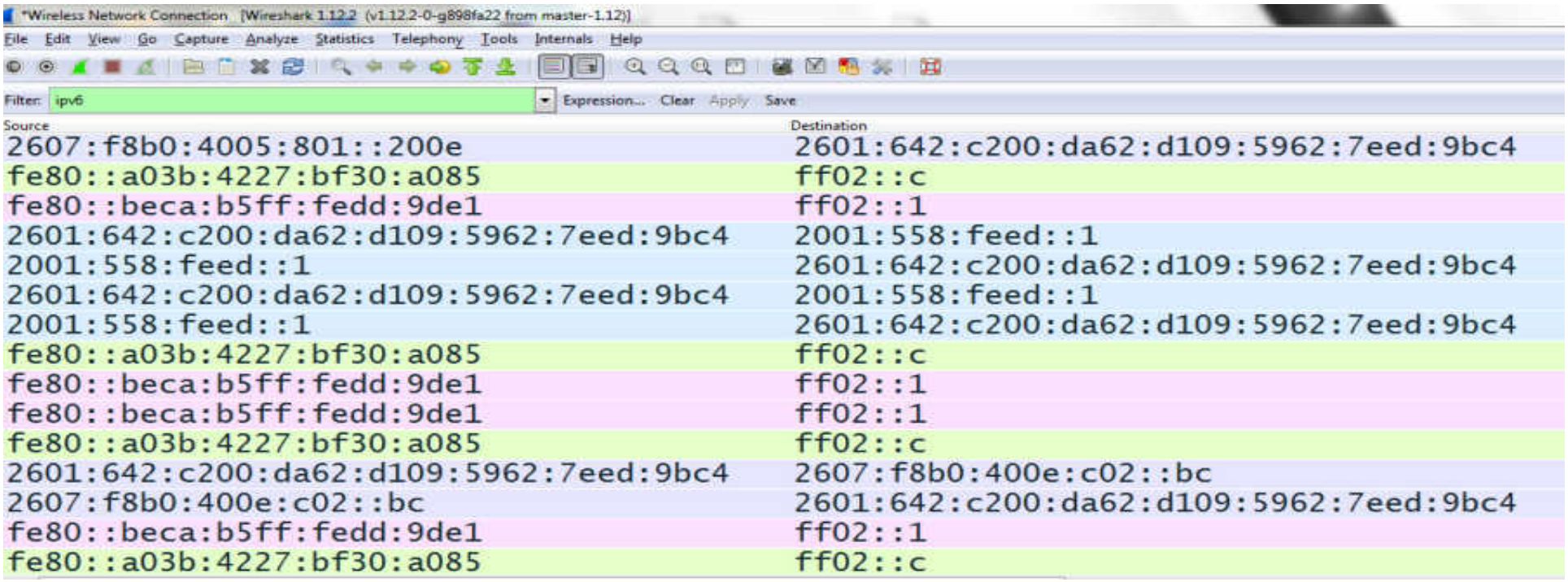
- Link-local or site-local
- Never routed outside a company or link
- Start with hex FE then 8 to F (1111 1110 1)

FE8n – FEFn = Private Addresses

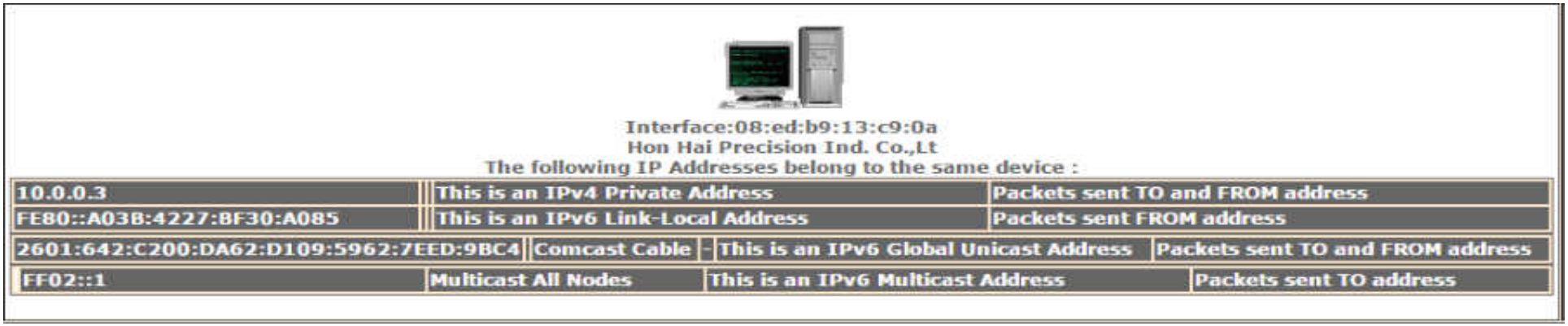
- Most common: FE80 (link-local)



Let’s take a trace!



Dual Stack Mode



Interface:08:ed:b9:13:c9:0a
Hon Hai Precision Ind. Co.,Lt
The following IP Addresses belong to the same device :

10.0.0.3	This is an IPv4 Private Address		Packets sent TO and FROM address
FE80::A03B:4227:BF30:A085	This is an IPv6 Link-Local Address		Packets sent FROM address
2601:642:C200:DA62:D109:5962:7EED:9BC4	Comcast Cable -	This is an IPv6 Global Unicast Address	Packets sent TO and FROM address
FF02::1	Multicast All Nodes	This is an IPv6 Multicast Address	Packets sent TO address

Dual stack mode makes it even more necessary to deduce configuration.

Router Advertisement

```
⊟ Ethernet II, Src: ArrisGro_dd:9d:e1 (bc:ca:b5:dd:9d:e1), Dst: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a)
  ⊞ Destination: HonHaiPr_13:c9:0a (08:ed:b9:13:c9:0a)
  ⊞ Source: ArrisGro_dd:9d:e1 (bc:ca:b5:dd:9d:e1)
    Type: IPv6 (0x86dd)
⊞ Internet Protocol Version 6, Src: fe80::beca:b5ff:fedd:9de1 (fe80::beca:b5ff:fedd:9de1), Dst: ff02::1
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xcb35 [correct]
    Cur hop limit: 64
  ⊞ Flags: 0x40
    Router lifetime (s): 1800
    Reachable time (ms): 3600000
    Retrans timer (ms): 1000
  ⊞ ICMPv6 Option (Prefix information : 2601:642:c200:da62::/64)
  ⊞ ICMPv6 Option (Recursive DNS Server 2001:558:feed::1)
  ⊞ ICMPv6 Option (Recursive DNS Server 2001:558:feed::2)
  ⊞ ICMPv6 Option (Source link-layer address : bc:ca:b5:dd:9d:e1)
```

- Source is link local of router
- Dest is multicast all nodes but L2 is our device!

What is multicast L2 for IPv6?

- Depends on medium
- Let’s take Ethernet:

- Start with x3333
- Then use last four bytes of the IPv6 multicast address

- For example, multicast address for DHCPv6 servers
- ff05::1:3
- becomes
- Ethernet MAC address 33-33-00-00-01-03

Ping to Multicast All Nodes (ff02::1)

Ping FF02::1 -n 10

ICMP Type	Packet	Number
128	Echo Request	10
129	Echo Reply	2,840
135	Neighbor Solicitation	578
136	Neighbor Advertisement	568

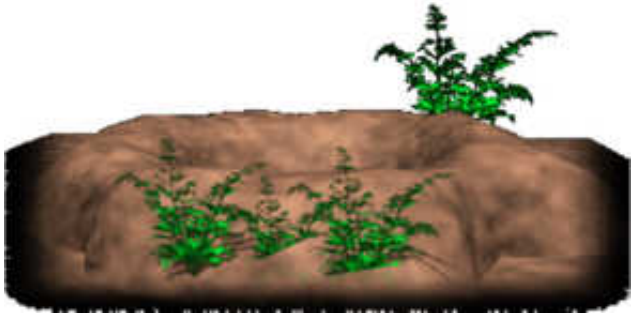
- What!!!
- Sent 10 received 2,840?

What Does Anonymous Proxy Do?

Changes your IP address

Why Anonymous Proxy?

- Privacy (NSA)
- Bypass legal restrictions on visiting certain web sites imposed by country or admin,
- Skip ads
- Malicious activity without having it be tracked back to you (spamming or attacking)



Who Uses Anonymous Proxy?

- Many people!
- Found on UTube:
  - Using Web Proxy Servers for Hacking
  - How to become anonymous online (VPN, TOR & Proxy)
  - Browsing with Tor: Online Anonymity to Outsmart the NSA - Tom Lowenthal

Who Provides Anonymous Proxy?

- Many, many servers!
- Free and paid services

HideMyAss - https://www.hidemyass.com/proxy
Proxify – http://proxify.com/p/
Ninja Clock – http://ninjacloak.com/
AnonyMouse - http://anonymouse.org/
AnonyMizer – http://www.anonymizer.com/
kProxy – http://www.kproxy.com/
BlewPass - http://www.blewpass.com/
Zfreez – http://zendproxy.com/
Vobas – http://www.vobas.com/
Don't Filter – http://www.dontfilter.us/

Problems with Anonymous Proxy

- The proxy server knows exactly what you are doing
- Have self-created a man-in-the-middle situation!
- Who are these guys?

Sample Anonymous Proxy

Sample Anonymous Proxy Servers

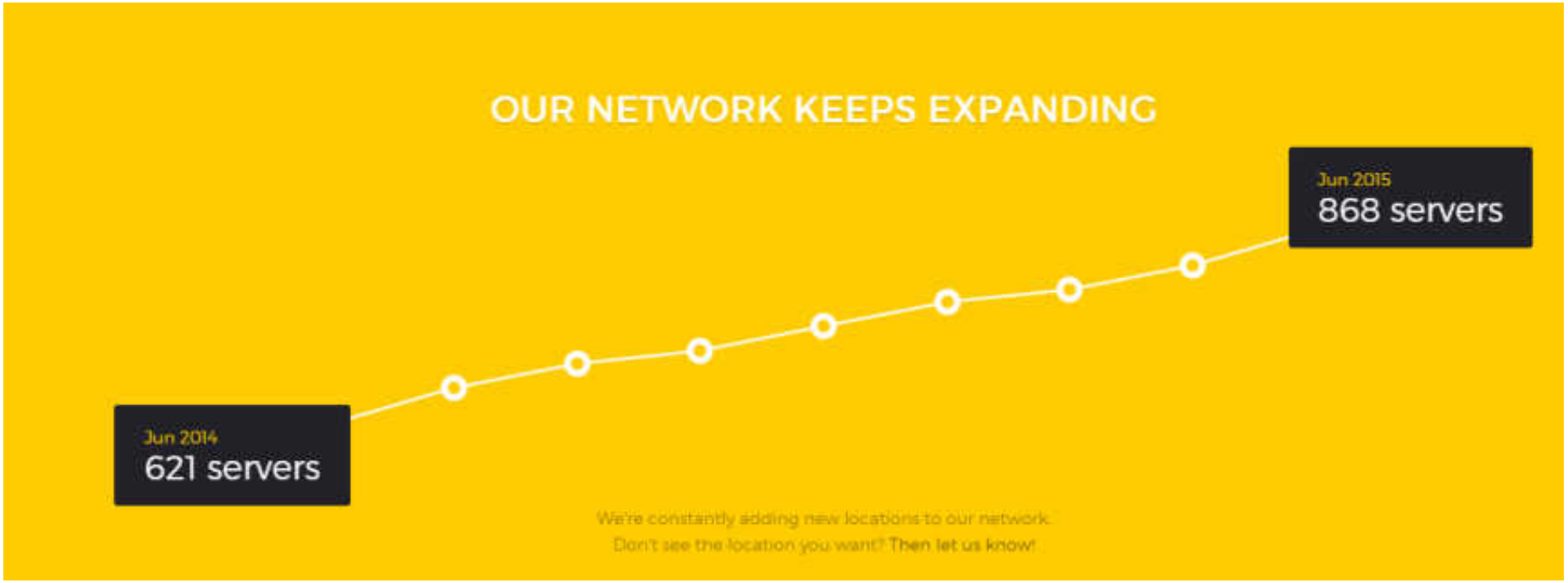
HIDE MY ASS!

VPN | How VPN works | Pricing | Tools & Contact | Help | English

OUR VPN SERVERS

Search locations	Servers	Total IPs	
Africa	22	2,341	SHOW
Asia	48	6,872	HIDE
Afghanistan	1	252	SHOW
Bahrain	1	252	SHOW
Bangladesh	1	252	SHOW

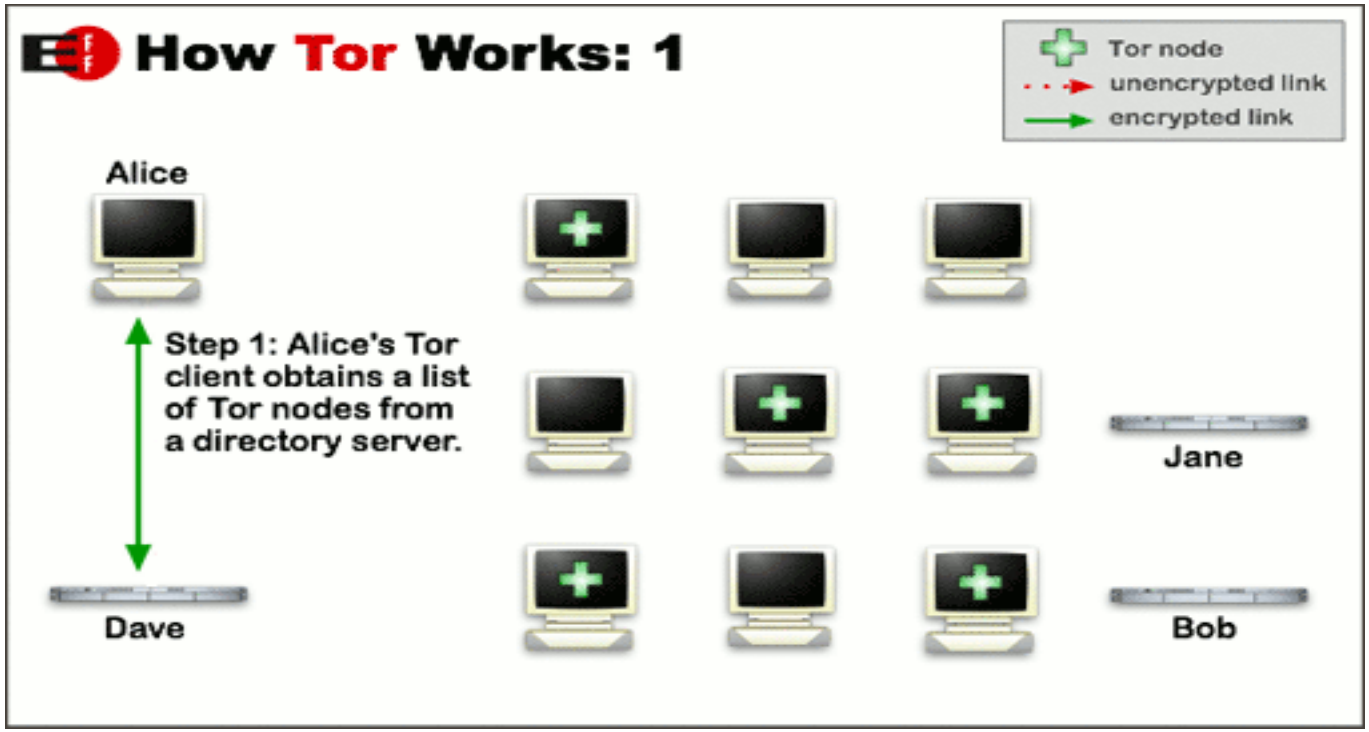
New servers every day!



TOR

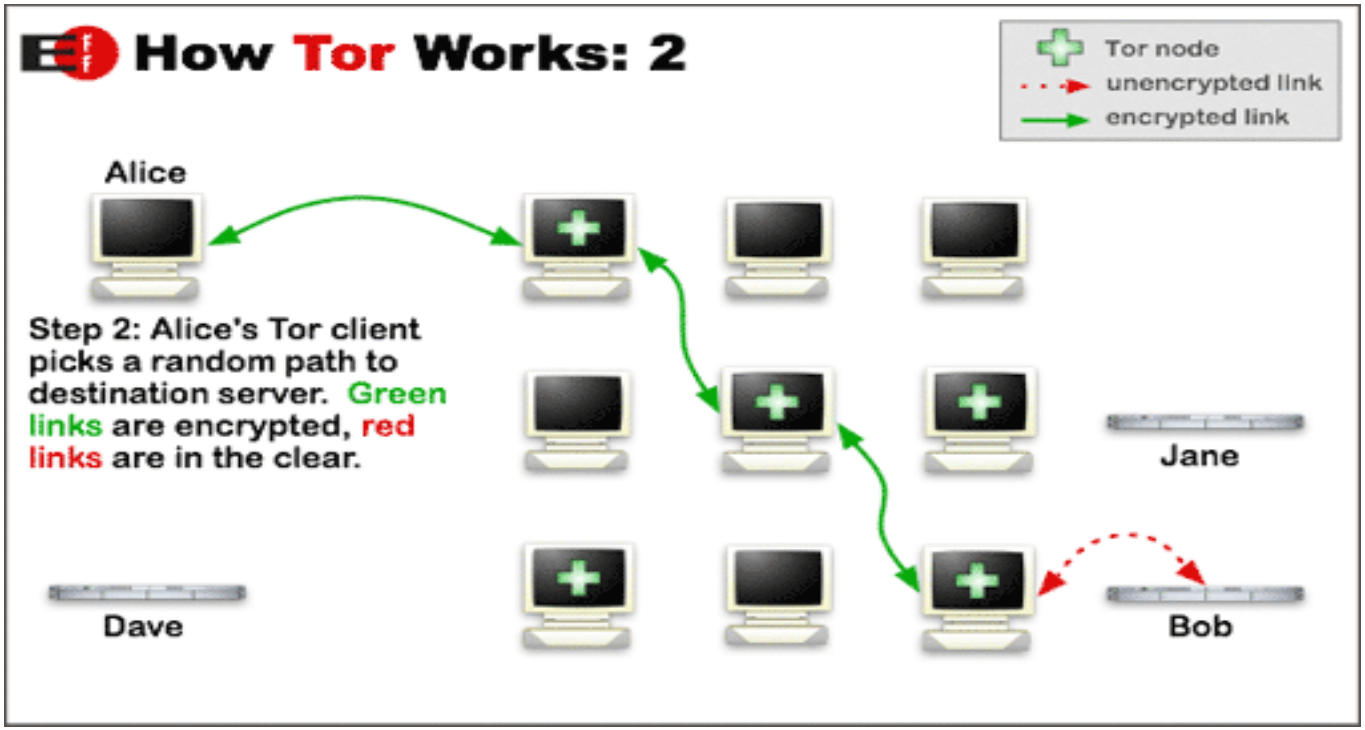
- www.torproject.org
- The Onion Routing network
- Started by U.S. Naval Research Library
- Network of virtual tunnels

How Does TOR Work?



www.tor.org

TOR Path



www.tor.org

TOR Browser

- No proxies involved
- Local to your network

Date	Time	System	Location	Host Name/Web Page/Referrer
27 Jan	06:45:45	Firefox 31.0 Win7	? Anonymous Proxy	Boston University (204.8.156.142) [Label IP Address] www.insidethestack.com/ (No referring link)

Summary

- Integrating Layer 2 - Layer 3 information as well as DNS names can be quite helpful!

- Addresses may not be who you think they are!

Contact Info

- Nalini Elkins
- Nalini.elkins@insidethestack.com
- (831) 659-8360

- Love to hear from you!