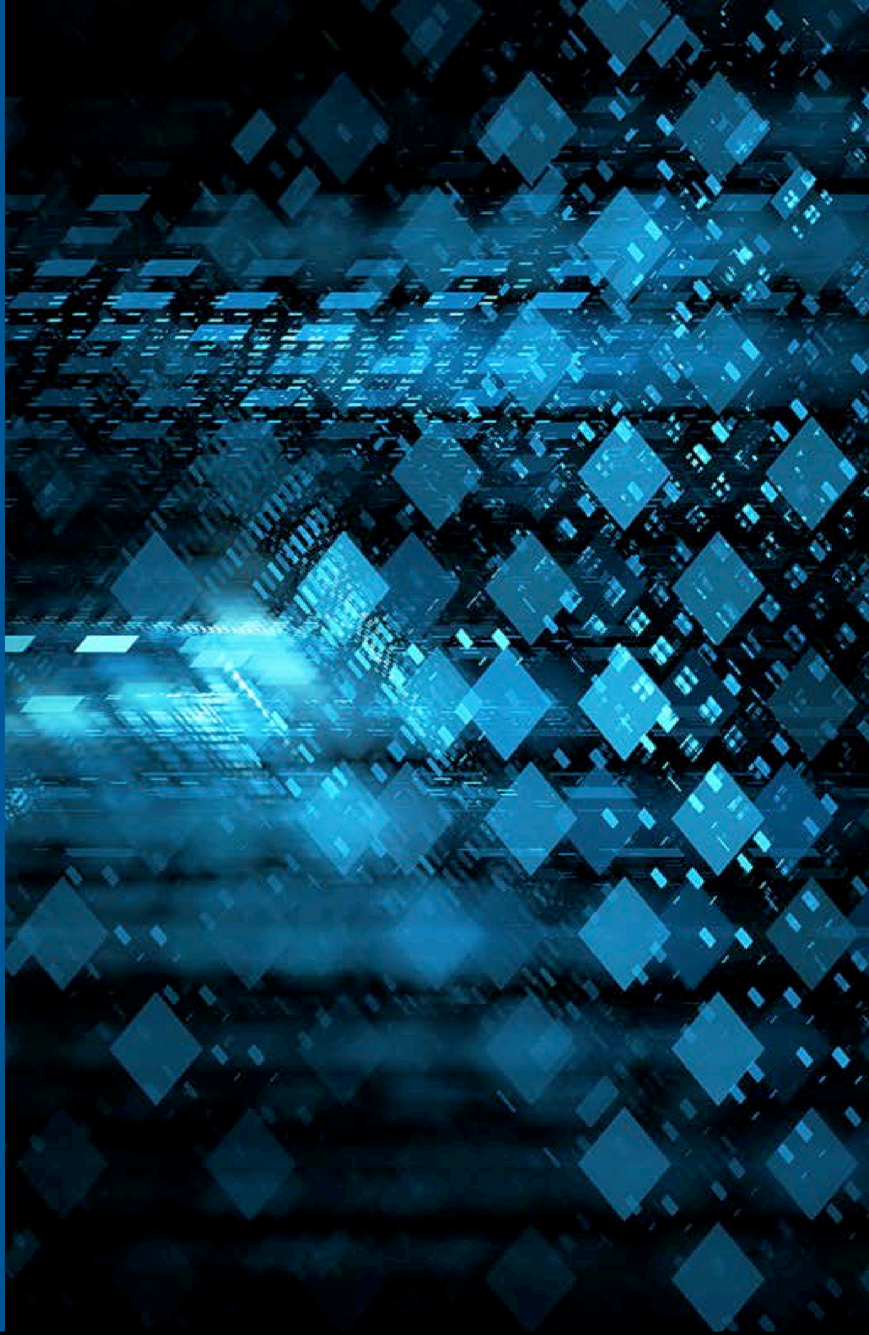
DODGING A BULLET: Avoiding the new security issues in IPv6 DHCP

October 19-20, 2017

Joseph Mayes
CMU Software Engineering Institute
CMU Heinz College

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

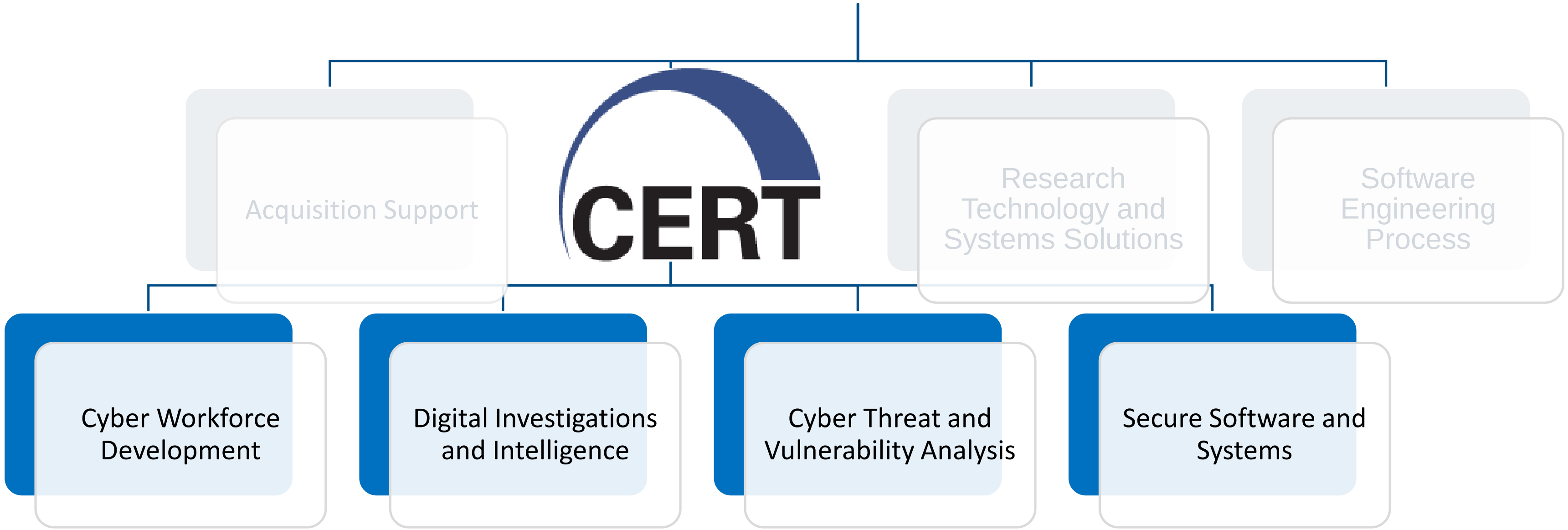
NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM17-0706

CERT ® Intro

Carnegie Mellon

Software Engineering Institute



Acquisition Support

CERT

Research Technology and Systems Solutions

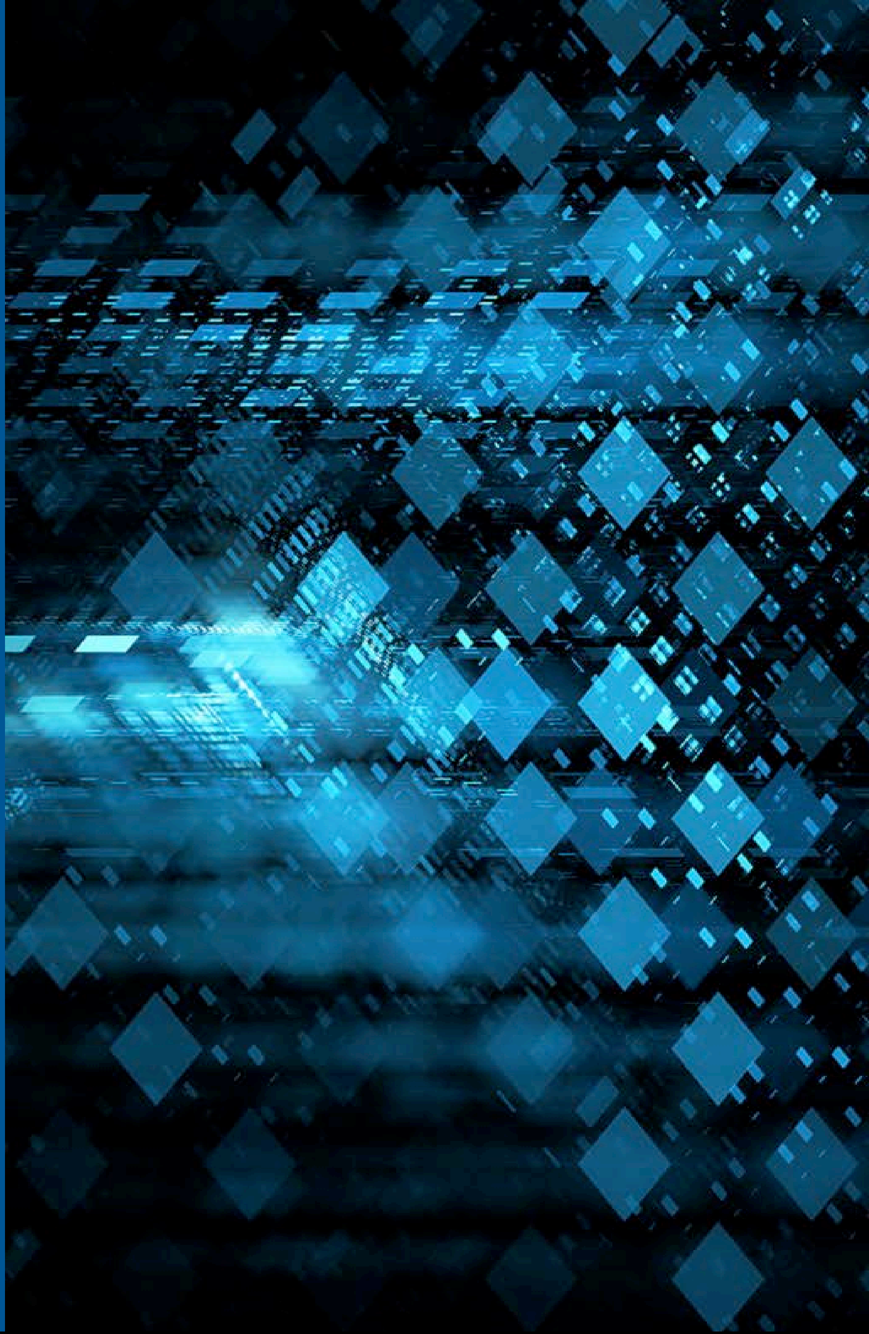
Software Engineering Process

Cyber Workforce Development

Digital Investigations and Intelligence

Cyber Threat and Vulnerability Analysis

Secure Software and Systems



AGENDA:

Part 1: Introduction

Part 2: IPv6 new technologies

Part 3: IPv6 new vulnerabilities

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

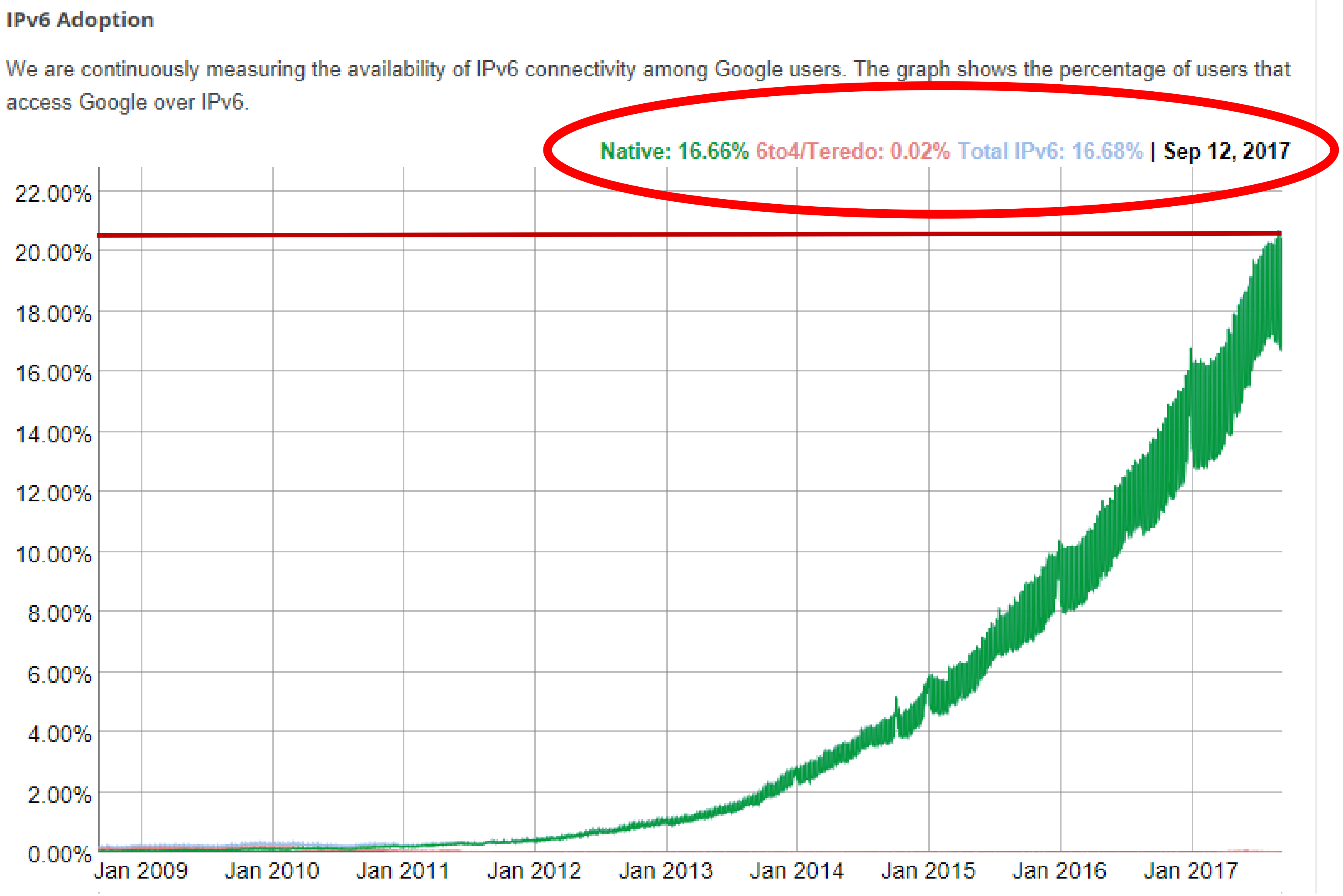
INTRODUCTION: Is IPv6 still right around the corner?

In fact, we have already turned the corner!
The time to learn IPv6 security techniques IPv6 is NOW!

Exponential increases in IPv6 adoption

From Google:
IPv6 use has doubled every year since 2012

Google reports show peaks of greater than 20% of all Google users



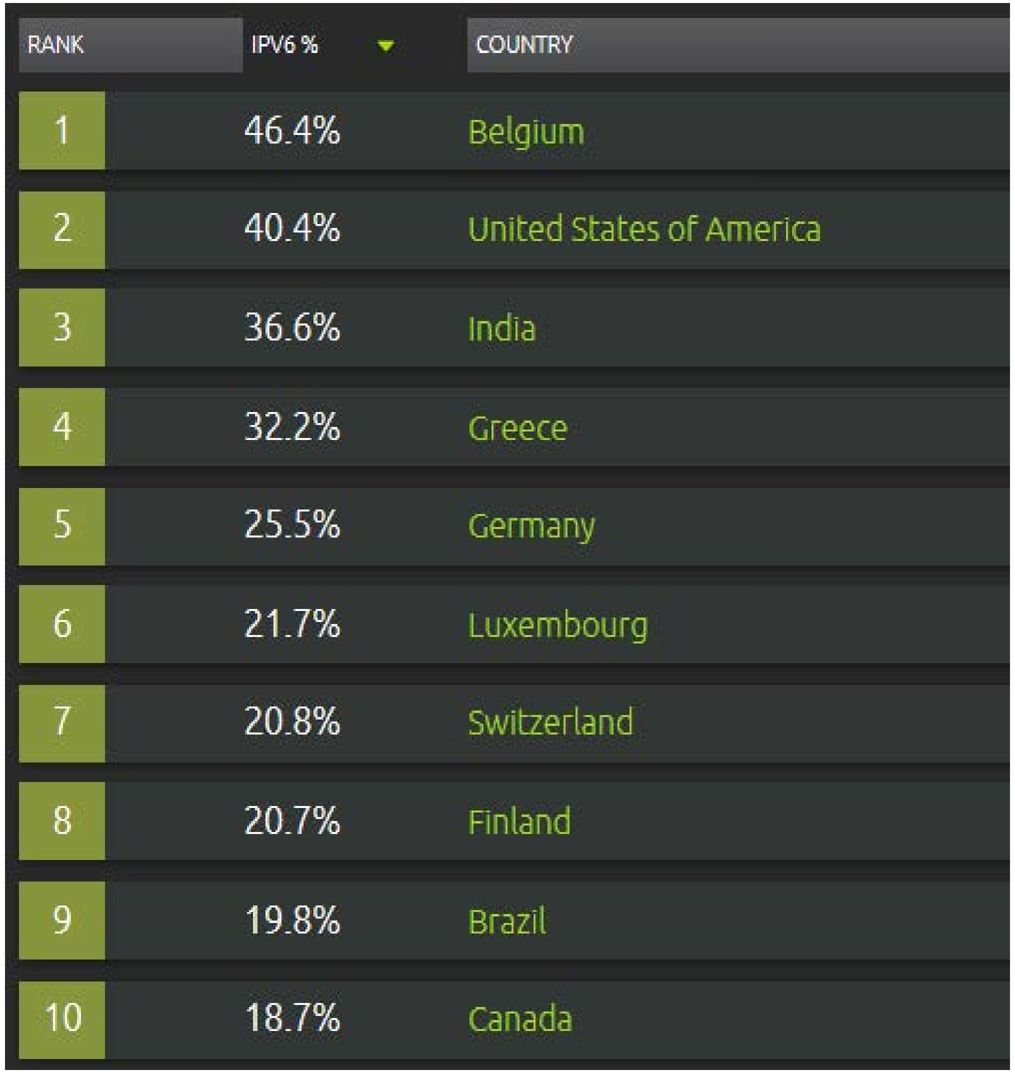
IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.

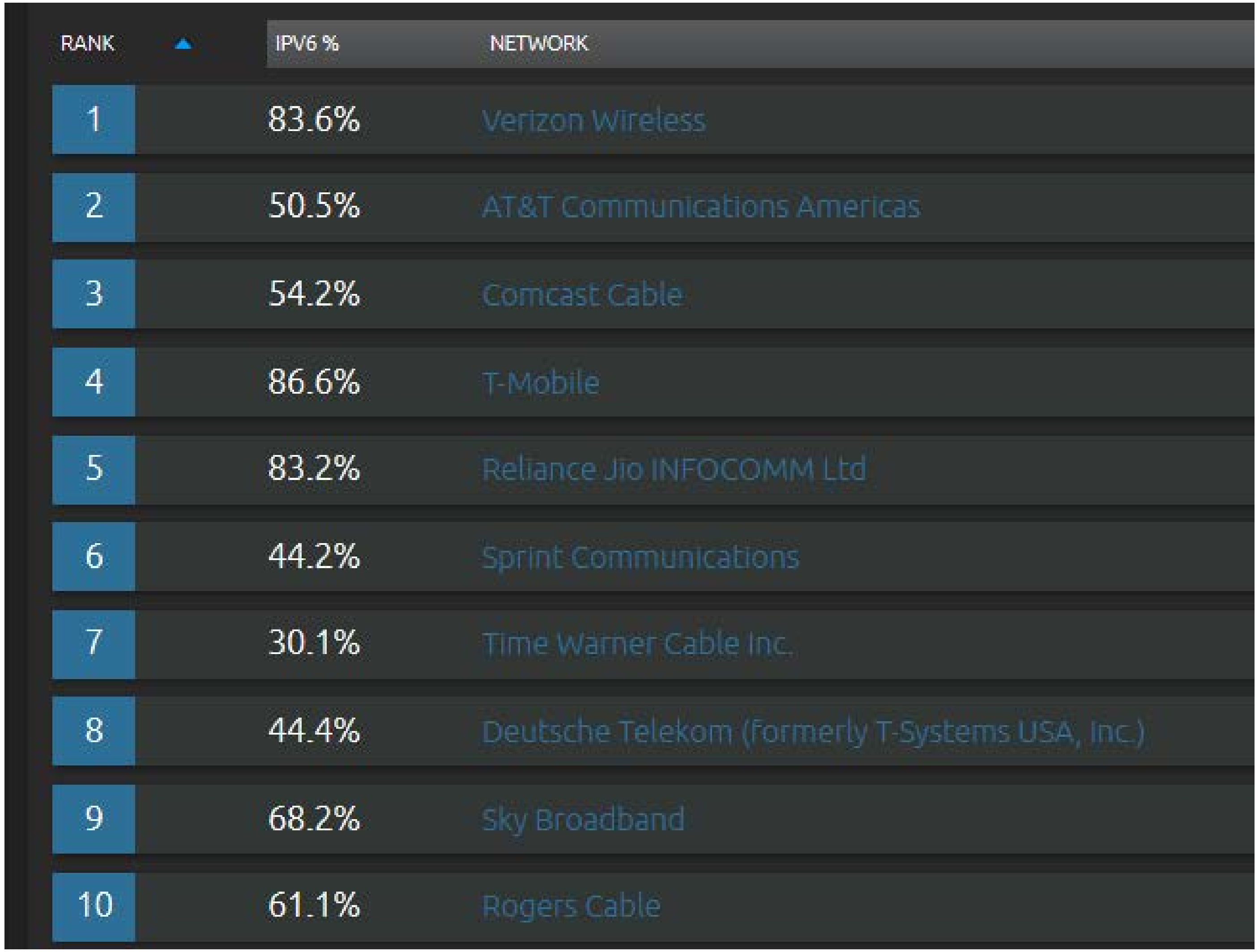
Native: 16.66% 6to4/Teredo: 0.02% Total IPv6: 16.68% | Sep 12, 2017

(Google graph, Sept. 2017)

So who’s doing all this IPv6 traffic? *(tables from Akamai, 2017)*

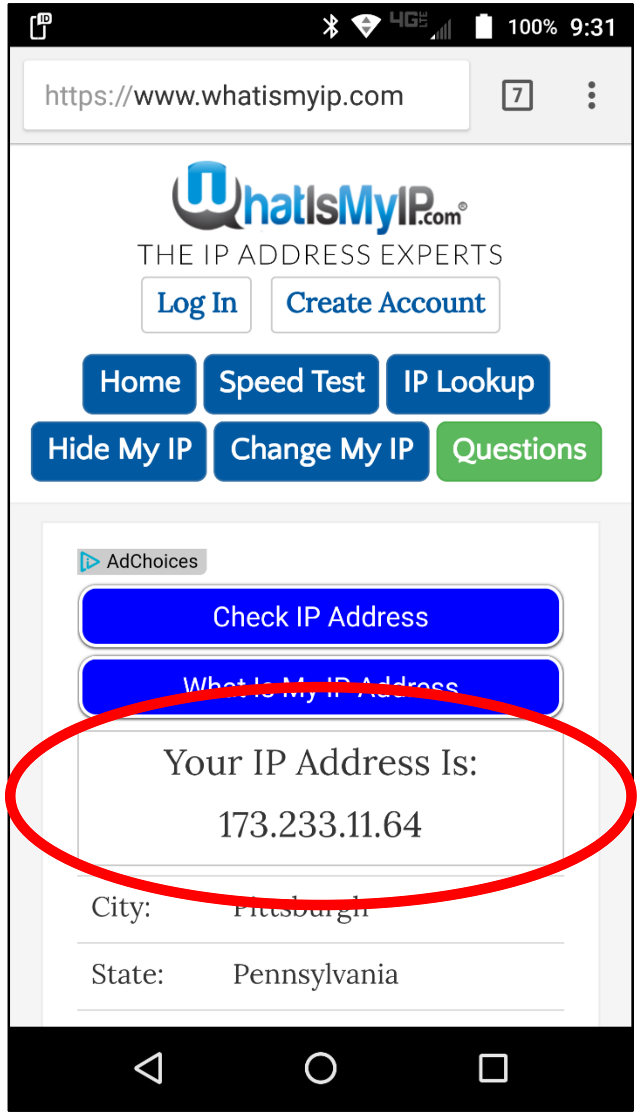


RANK	IPV6 % ▼	COUNTRY
1	46.4%	Belgium
2	40.4%	United States of America
3	36.6%	India
4	32.2%	Greece
5	25.5%	Germany
6	21.7%	Luxembourg
7	20.8%	Switzerland
8	20.7%	Finland
9	19.8%	Brazil
10	18.7%	Canada



RANK ▲	IPV6 %	NETWORK
1	83.6%	Verizon Wireless
2	50.5%	AT&T Communications Americas
3	54.2%	Comcast Cable
4	86.6%	T-Mobile
5	83.2%	Reliance Jio INFOCOMM Ltd
6	44.2%	Sprint Communications
7	30.1%	Time Warner Cable Inc.
8	44.4%	Deutsche Telekom (formerly T-Systems USA, Inc.)
9	68.2%	Sky Broadband
10	61.1%	Rogers Cable

My smartphone
on Wi-Fi…



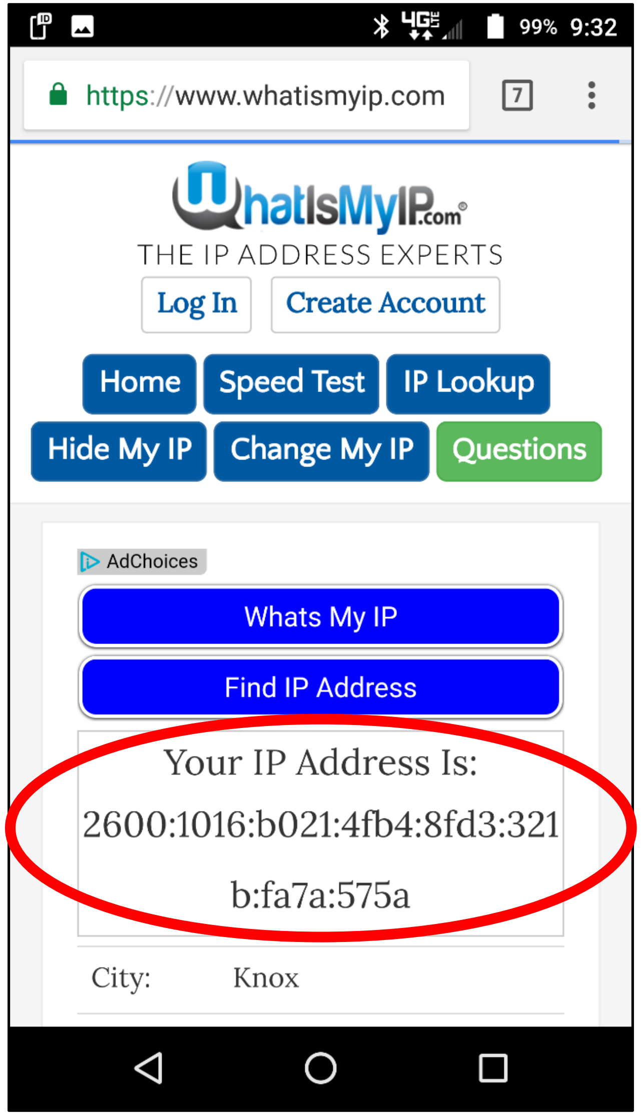
Your IP Address Is:

173.233.11.64

City: Pittsburgh

State: Pennsylvania

My smartphone
on Verizon 4G…



Your IP Address Is:

2600:1016:b021:4fb4:8fd3:321b:fa7a:575a

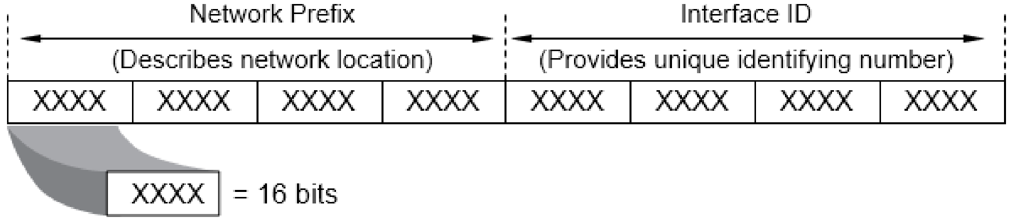
City: Knox

Software Engineering Institute | Carnegie Mellon University

IPv6 TECHNOLOGIES: Significant Differences Compared to IPv4

It’s not just longer addresses!

128-bit IPv6 address



Network Prefix (Describes network location)				Interface ID (Provides unique identifying number)			
XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX	XXXX

XXXX = 16 bits

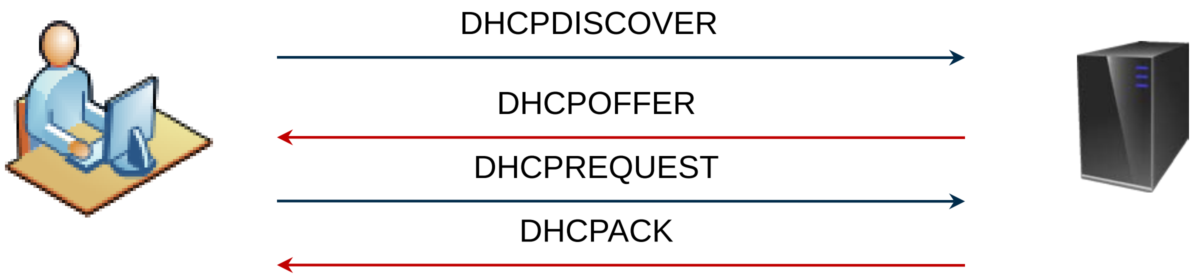
- New Protocols
  - DNSv6 support
  - Address Autoconfiguration options
  - IPv6-capable host systems
  - IPv6-capable networking
  - IPv6 routing
  - IPv6-capable security systems and processes

IPv4 DHCP (review)

Provides address assignment when requested by IP host

DHCP is a client-server 4-step process

- DHCP communication between client and DHCP server(s)
  - Discover – client broadcasts request (UDP port 67)
  - Offer – server(s) reply with potential address (UDP port 68)
  - Request – client accepts offer from 1st server
  - Acknowledgement – selected server provides IP address and other configuration parameters



IPv6 Broadcasts, multicasts and DHCP

IPv6 does not support broadcast addresses or broadcast transmissions

- This makes IPv6 DHCP operate differently than IPv4

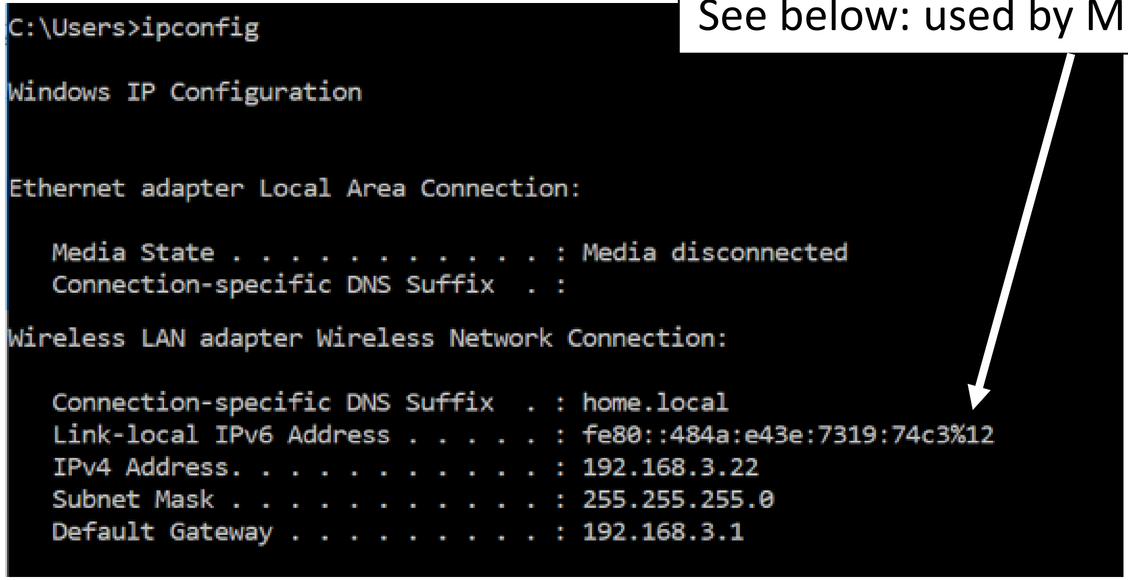
IPv6 use link-local multicast addresses instead

- Multicast range is FF00::/8
- DHCPv6 uses multicasts communication
  - FF02::2 for Router Solicitations from hosts
    - reserved for communication to *All DHCPv6 Relay Agents and Servers*
  - FF02::1 for Router Advertisements (RAs) to DHCP clients
  - Routers and relay agents listen on UDP port 547, while clients listen on UDP port 546
  - DHCP relay agents convert multicast traffic to unicast traffic to send to remote DHCP servers

IPv6 addresses – Link-Local Addresses

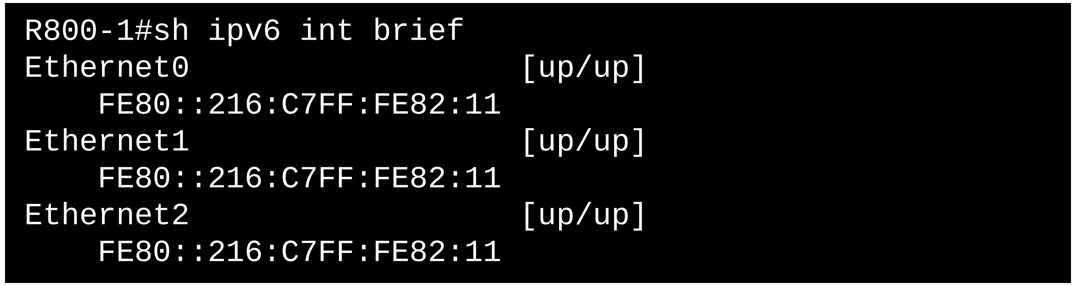
- Link-Local (FE80::/10)
  - Locally-generated, but can be statically set (in most systems)
  - Absolutely not routable (unlike 169.254.0.0 in IPv4)
  - EVERY HOST will have an FE80::/10 address, with or without DHCP
    - Nodes also join additional default multicast groups (varies by node type)

A %nn appended to the end of the address is a ‘zone’ or ‘scope’ identifier
See below: used by Microsoft to identify individual NICs



```
C:\Users>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . : home.local
   Link-local IPv6 Address . . . . . : fe80::484a:e43e:7319:74c3%12
   IPv4 Address. . . . . . . . . . . : 192.168.3.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.3.1
```

Question: what’s unusual here?



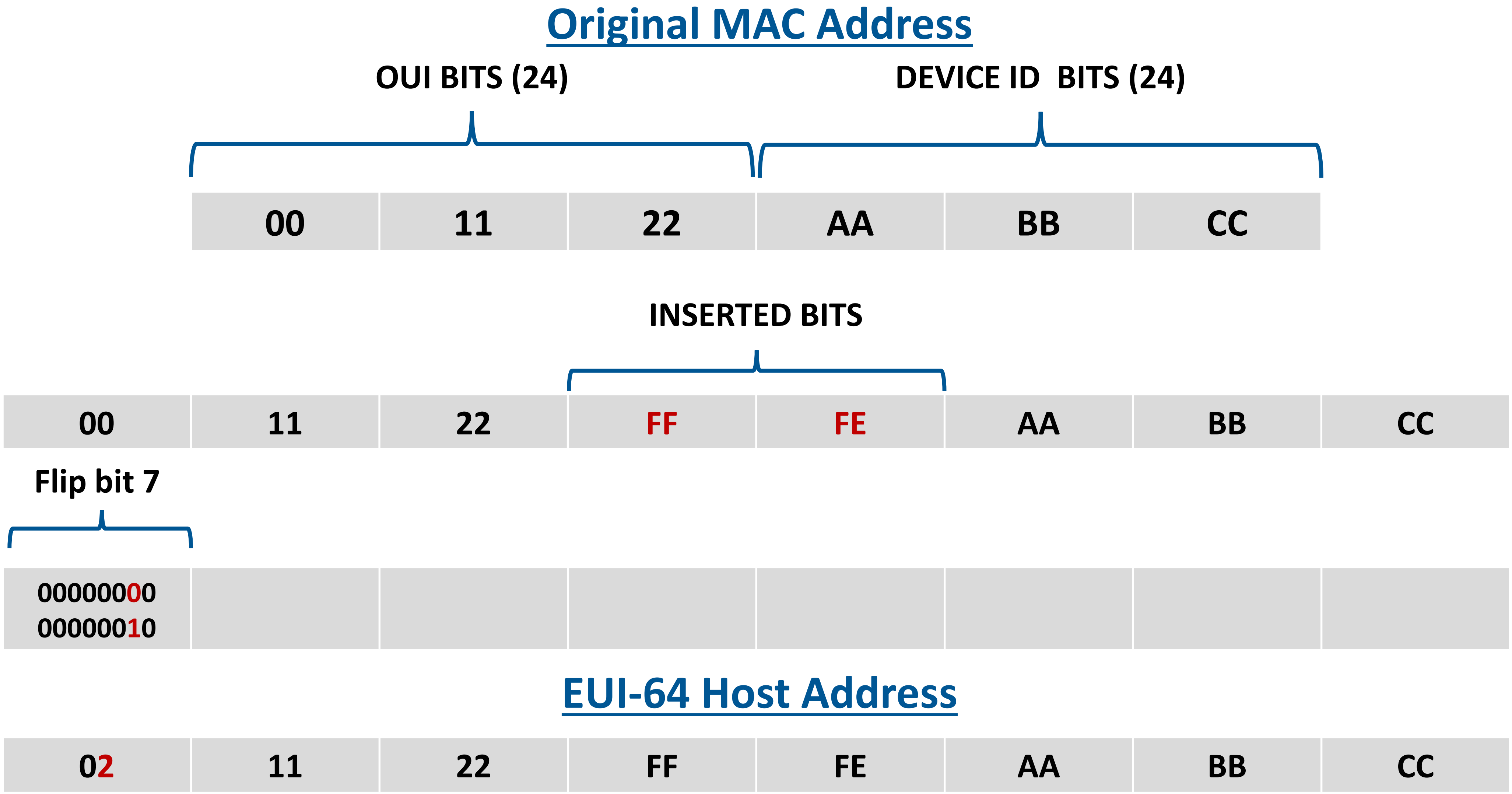
```
R800-1#sh ipv6 int brief
Ethernet0                    [up/up]
    FE80::216:C7FF:FE82:11
Ethernet1                    [up/up]
    FE80::216:C7FF:FE82:11
Ethernet2                    [up/up]
    FE80::216:C7FF:FE82:11
```

Link-Local Address host bit assignment and EUI-64

IPv6 does not use ARP requests / ARP replies to learn destination MAC addresses

- Each system self-assigns a link-local (FE80::/10) address
  - The 64 host bits are derived from the host's MAC address (if using the EUI-64 protocol)
    - The MAC address (48 bits) is used, with FF:FE inserted after the 24 OUI bits
      - For MAC is **00:11:22:AA:BB:CC**, the result would be **00:11:22:FF:FE:AA:BB:CC**
    - Finally, the 7th bit (from the left) is flipped from 0 to 1 to indicate a universal address type
      - So the 'Modified EUI-64' address would be **02:11:22:FF:FE:AA:BB:CC**
  - The system then sends a Neighbor Solicitation to ensure the address is link-unique
  - If unique, the system then sends a Neighbor Advertisement multicast on the link
  - (Neighbor Solicitations can also be used for additional host discovery needs)
- *NOTE: IPv6 management messages are sent using IPv6 ICMP packets*

EUI-64 Address Construction



Original MAC Address

OUI BITS (24)

DEVICE ID BITS (24)

00	11	22	AA	BB	CC

INSERTED BITS

00	11	22	FF	FE	AA	BB	CC

Flip bit 7

00000000 00000010							

EUI-64 Host Address

02	11	22	FF	FE	AA	BB	CC

IPv6 addresses – Static Configuration and Autoconfiguration

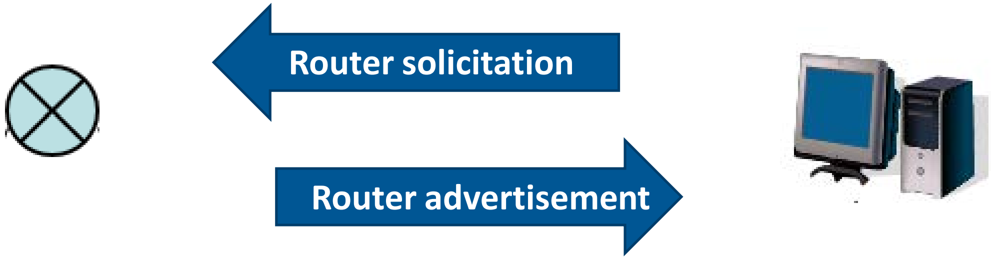
- Global Unicast addresses (2000::/3)
  - Can be statically assigned
- **Multiple methods for dynamic assignment, including**
  - Stateless Address Autoconfiguration (SLAAC)
  - SLAAC with Stateless DHCPv6
  - Stateful DHCPv6
  - DHCPv6-PD (with prefix designation)

- Router Advertisements (RAs) send flags indicating autoconfiguration parameters

- IPv6 Global Unicast addresses do not need Network Address Translation (NAT)

Router Advertisements

- Usually begins with host sending a Router Solicitation (FF02::2, UDP port 547)
- Router replies with a router Advertisement (FF02::1, UDP port 546)
  - The RA contains 3 flags:
    - A-bit (*Autonomous Address Configuration*)– default to ON (1)
    - M-bit (*Managed* [or stateful])– default to OFF (0)
    - O-bit (*Other* [signifies other information available])– default to OFF
  - Modifying these flags signals how the host should configure its address



Setting Router Advertisement Flags (Cisco Router)

Enabling IPv6 (enables IPv6 Router Advertisements)

```
Router#(config)ipv6 unicast-routing
interface Serial0/0
         no ip address
         ipv6 address 2010:AB8:0:1::1/64
         ipv6 enable
```

A-bit (*Autonomous Address Configuration*)– default is ON; this command turns A-bit OFF

```
         ipv6 nd prefix prefix/prefix-length no-autoconfig
```

M-bit (Managed [or stateful])– default to OFF (0); this command turns M-bit to ON

```
         ipv6 nd managed-config-flag
```

O-bit (Other [signifies other information available])– default to OFF; this command turns O-bit to ON

```
         ipv6 nd other-config-flag
```

Autoconfiguration with SLAAC (IPv6 default)

Stateless Address Autoconfiguration (SLAAC) (RFC 4862, obsoleting RFC 2462)

- Requires a valid Link-Local address already bound to the interface
    - A-bit (*Autonomous Address Configuration*)– default to ON (1)
    - M-bit (*Managed* [or stateful])– default to OFF (0)
    - O-bit (*Other* [signifies other information available])– default to OFF

- This default behavior instructs the host to
    - learn GUA network prefix and default gateway from router
    - Create host bits using EUI-64 process
- The address is considered ‘stateless’ because the address is not centrally managed

SLAAC (plus DNS entries)

SLAAC plus stateless DNS configuration info (RFC 6106 [deprecated] and 8106)

- Must meet all the previously-described requirements for SLAAC
- The DNS information is added to the router advertisement
  - It can provide DNS addresses directly
  - It can also direct the host to search vai multicast for Recursive DNS Servers (RDNSS)
    - RFC4861
    - Multicast address FF02::FB
    - Enabled using the following commands (at the router interface level)

```
ipv6 nd ra dns server [address] [lifetime in seconds]
```

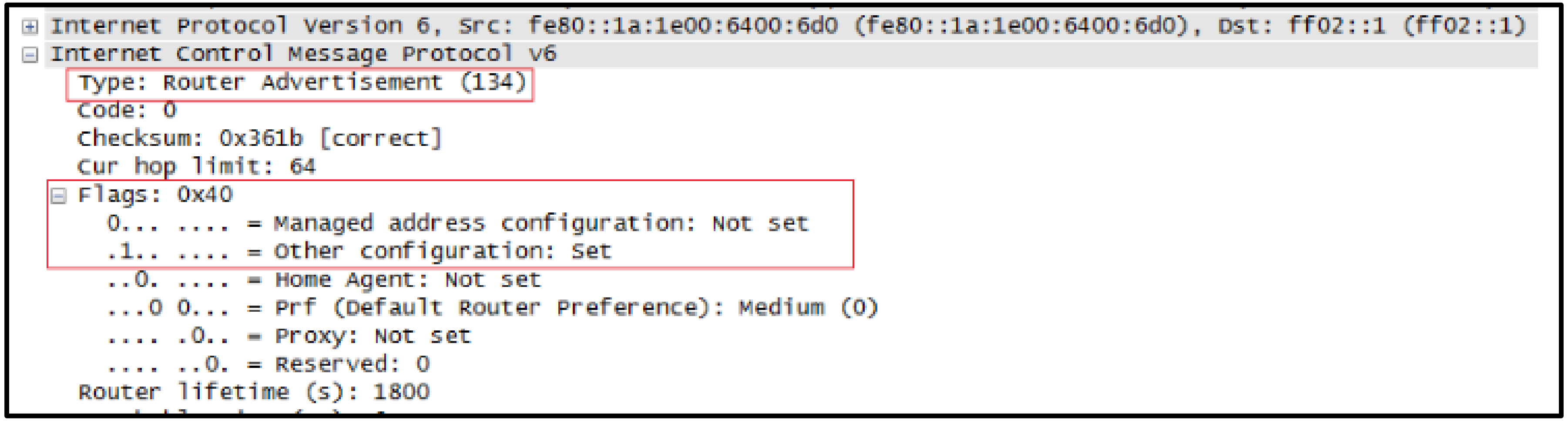
  - The RA can also advertise default domain names

- This RFC has not been universally adopted by client systems

Autoconfiguration with SLAAC (plus DNS entries)

SLAAC plus stateless DNS configuration info (RFC 6106 [deprecated] and 8106)

- Must meet all the previously-described requirements for SLAAC
- The RA flags change, turning the O-bit to 1:
  - This behavior instructs the host to query for DNS providers
    - DNS entries can be configured on the gateway router or via IPv6 DHCP server
    - When both are present, the RFC gives precedence to the DHCP server
    - As long as the M-bit is still OFF, the node address will still be from SLAAC



```
⊞ Internet Protocol Version 6, Src: fe80::1a:1e00:6400:6d0 (fe80::1a:1e00:6400:6d0), Dst: ff02::1 (ff02::1)
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x361b [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x40
      0... .... = Managed address configuration: Not set
      .1.. .... = Other configuration: Set
      ..0. .... = Home Agent: Not set
      ...0 0... = Prf (Default Router Preference): Medium (0)
      .... .0.. = Proxy: Not set
      .... ..0. = Reserved: 0
    Router lifetime (s): 1800
```

Stateful DHCP (RFC 3315)

Similar, but not identical to IPv4 DHCP

Indicated by setting RA M-bit to ON

- System still receives RA first, for gateway, network and M-bit settings
- Stateful DHCP, as server tracks status of dynamically-assigned address
  - Desired behavior tracks host by DHCPv6 Unique Identified (DUID), not MAC address
- To learn additional scope settings, O-bit must also be set to ON

- Many systems will still also set a SLAAC address unless A-bit is turned OFF
  - If M-bit and A-bit both on, many systems will bind both addresses to NIC

DHCPv6-PD (RFC 3633)

Uses DHCP to pass additional address prefix designations to a DHCP client

- The client is almost exclusively a downstream router supporting downstream subnets
  - Can be used commercially, or can provide internal IPv6 subnets for home routers
  - Prefixes are requested by downstream router in its router solicitation
  - Upstream router must be configured to provide DHCP6-PD responses
- DHCP6-PD can be a stand-alone service, or can also provide stateful DHCP

```
ipv6 unicast-routing
ipv6 dhcp pool dhcpv6
!--- The DHCP pool is named "dhcpv6."
prefix-delegation pool dhcpv6-pool1 lifetime 1800 600
!--- The prefix delegation pool name is "dhcpv6-pool1."
dns-server 2001:DB8:3000:3000::42
domain-name example.com
!
interface Serial0/0
 no ip address
 ipv6 address 2010:AB8:0:1::1/64
 ipv6 enable
 ipv6 dhcp server dhcpv6
!--- designates this interface as a DHCP server
interface
ipv6 local pool dhcpv6-pool1 2001:DB8:1200::/40 48
!--- The prefix pool named dhcpv6-pool1 has a prefix of
length
!--- /40 from which it will delegate (sub)prefixes of
length /48.
```

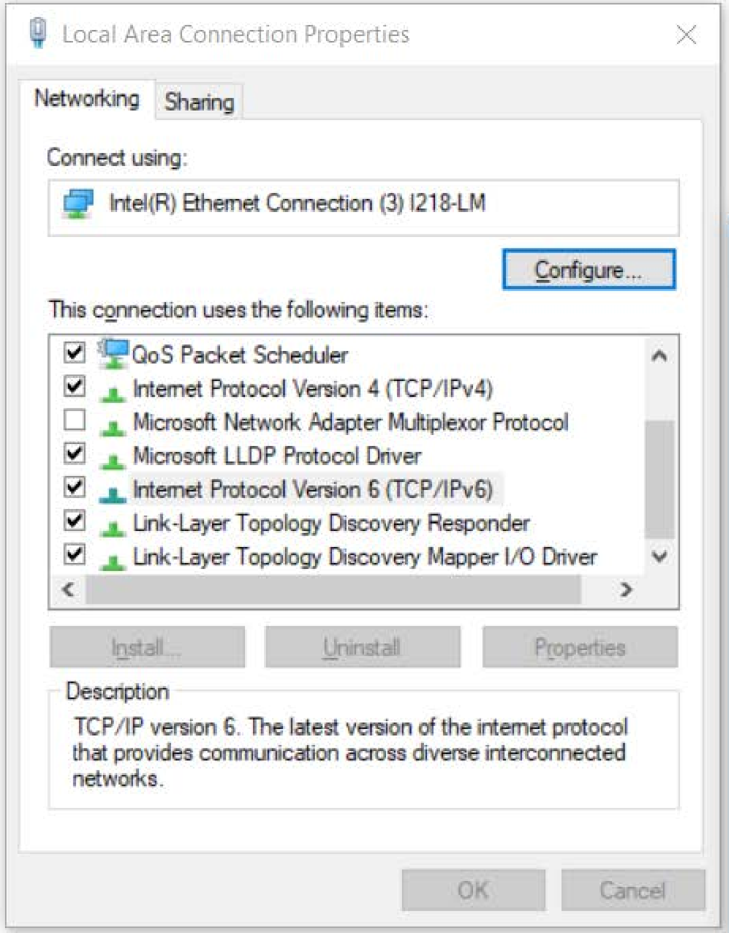
IPv6 autoconfiguration caveats

Some IPv6 clients do not support all IPv6 autoconfiguration features

Some IPv6 clients are programmed to ignore or modify autoconfiguration responses

- Some operating systems DO NOT use EUI-64 addressing for SLAAC
  - Instead, they generate random host address bits using RFC 4941
    - Windows Vista and later 'client' OSes
    - Windows Vista and later (and Mac Lion OS and later) also create 'temporary' dynamic addresses with RFC 4941-compliant addresses
      - Both systems use these 'temporary' address as the preferred address for outbound communication

IPv6 client configuration – Microsoft WIndows



Local Area Connection Properties

Connect using:

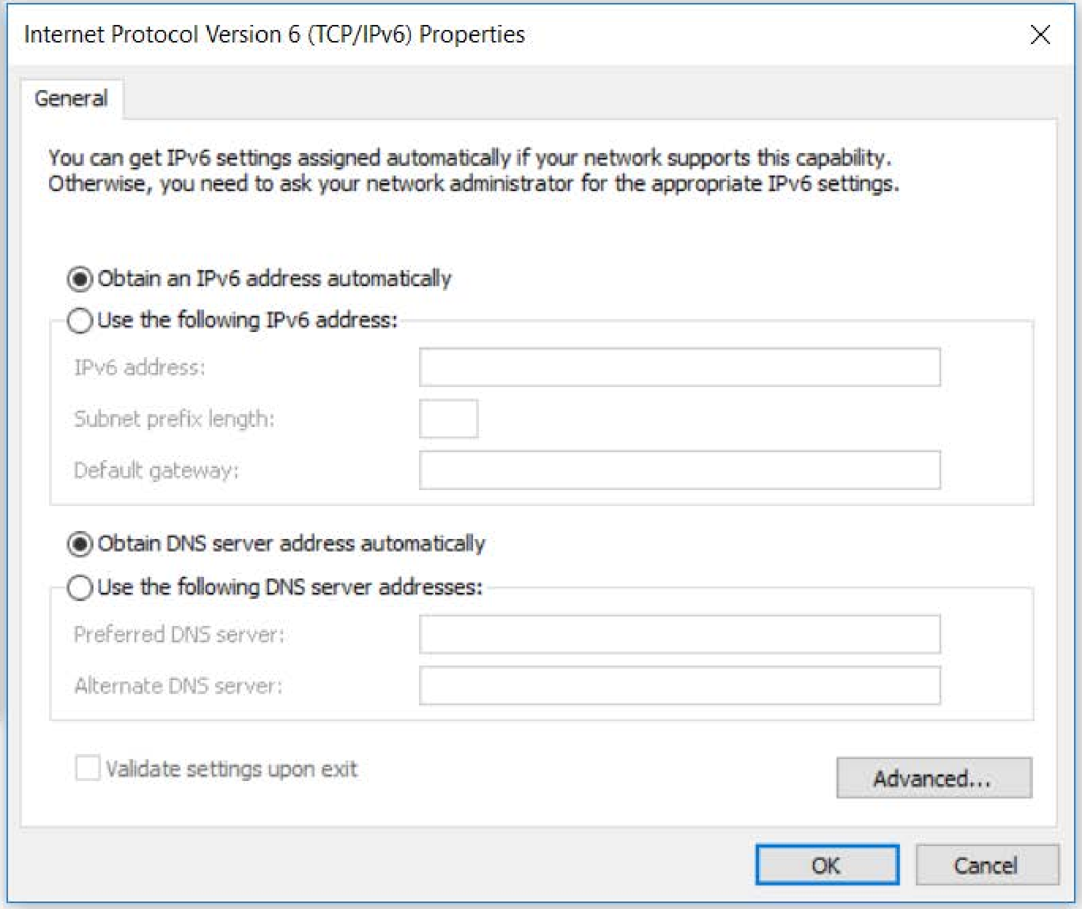
Intel(R) Ethernet Connection (3) I218-LM

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.



Internet Protocol Version 6 (TCP/IPv6) Properties

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

● Obtain DNS server address automatically

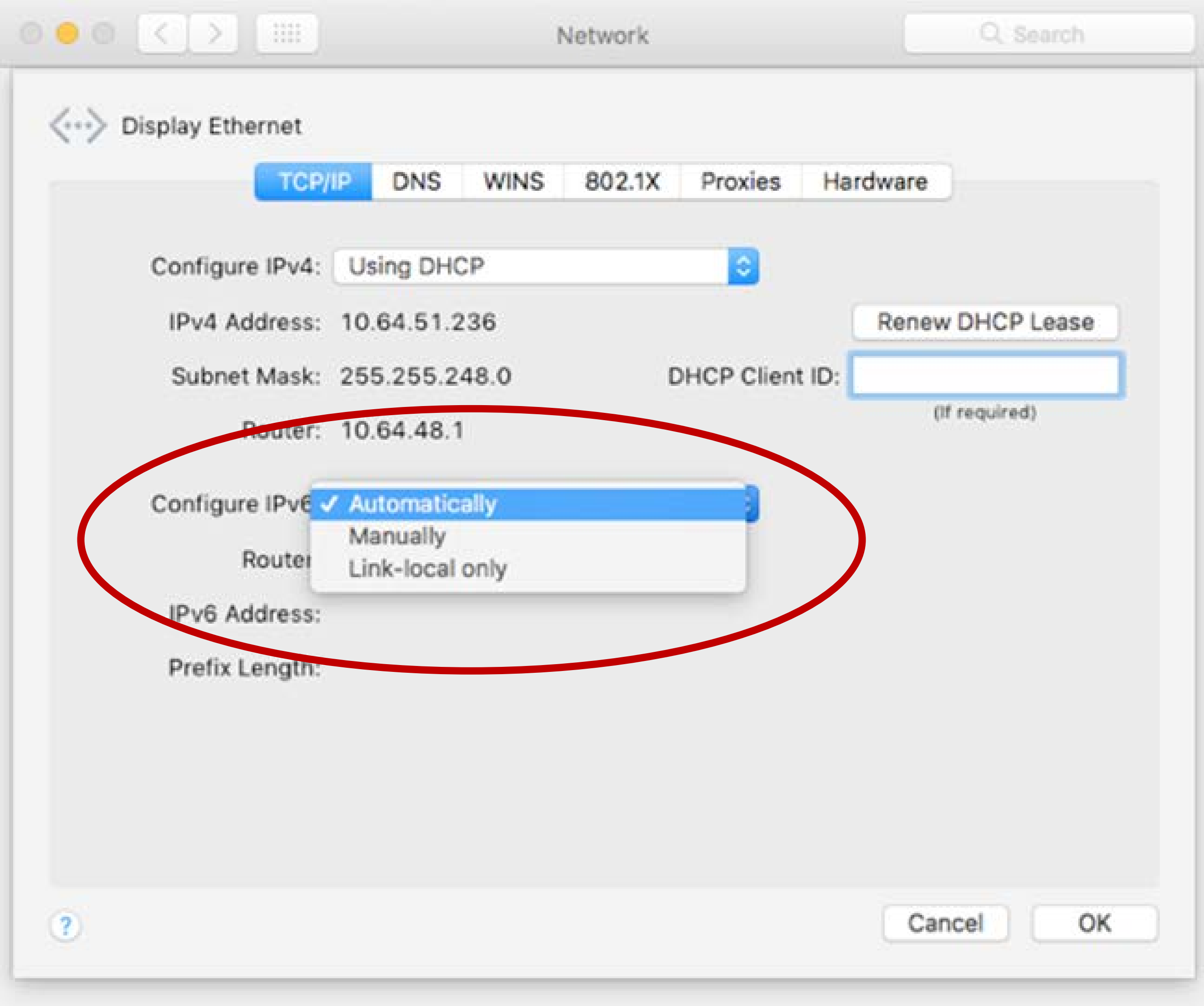
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

IPv6 client configuration – Apple MacIntosh



Network

Display Ethernet

Configure IPv4: Using DHCP

IPv4 Address: 10.64.51.236

Subnet Mask: 255.255.248.0

Router: 10.64.48.1

DHCP Client ID:

(If required)

Configure IPv6: ✓ Automatically

Manually

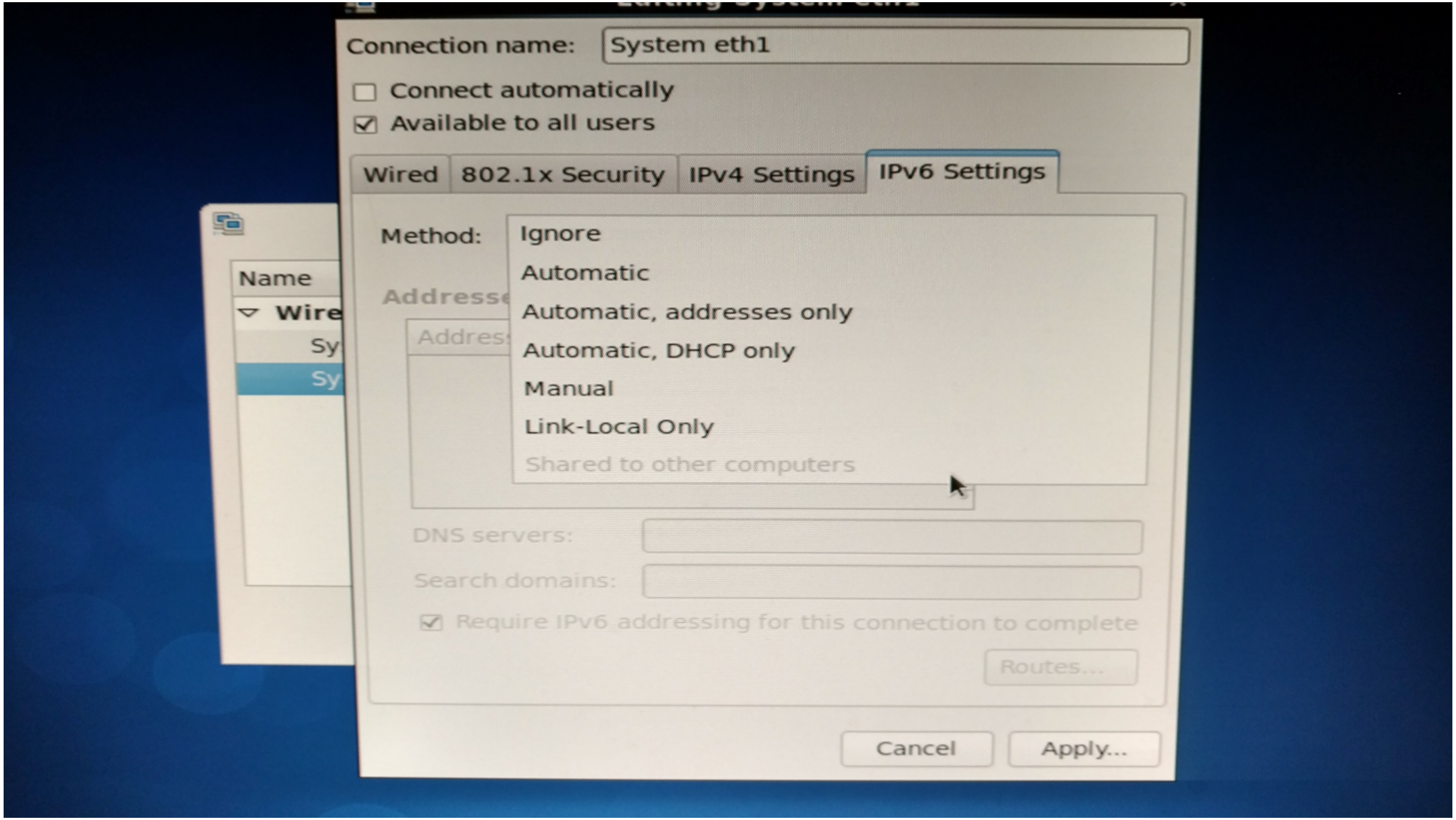
Link-local only

Router:

IPv6 Address:

Prefix Length:

IPv6 client configuration – Linux (CentOS 6; Red Hat open source)



Connection name: System eth1

□ Connect automatically

☑ Available to all users

IPv6 VULNERABILITIES: New Risks to Manage

NOTE: The listed vulnerabilities are limited to those related to IPv6 autoconfiguration and DHCPv6

- **The dangers of EUI-64 addressing**
- **IPv6 traffic you don’t recognize is there**
- **Spoofed ICMPv6 messages**
- **Manipulating IPv6 DNS support**
- **Duplicate Address Detection DOS**

EUI-64 vulnerabilities

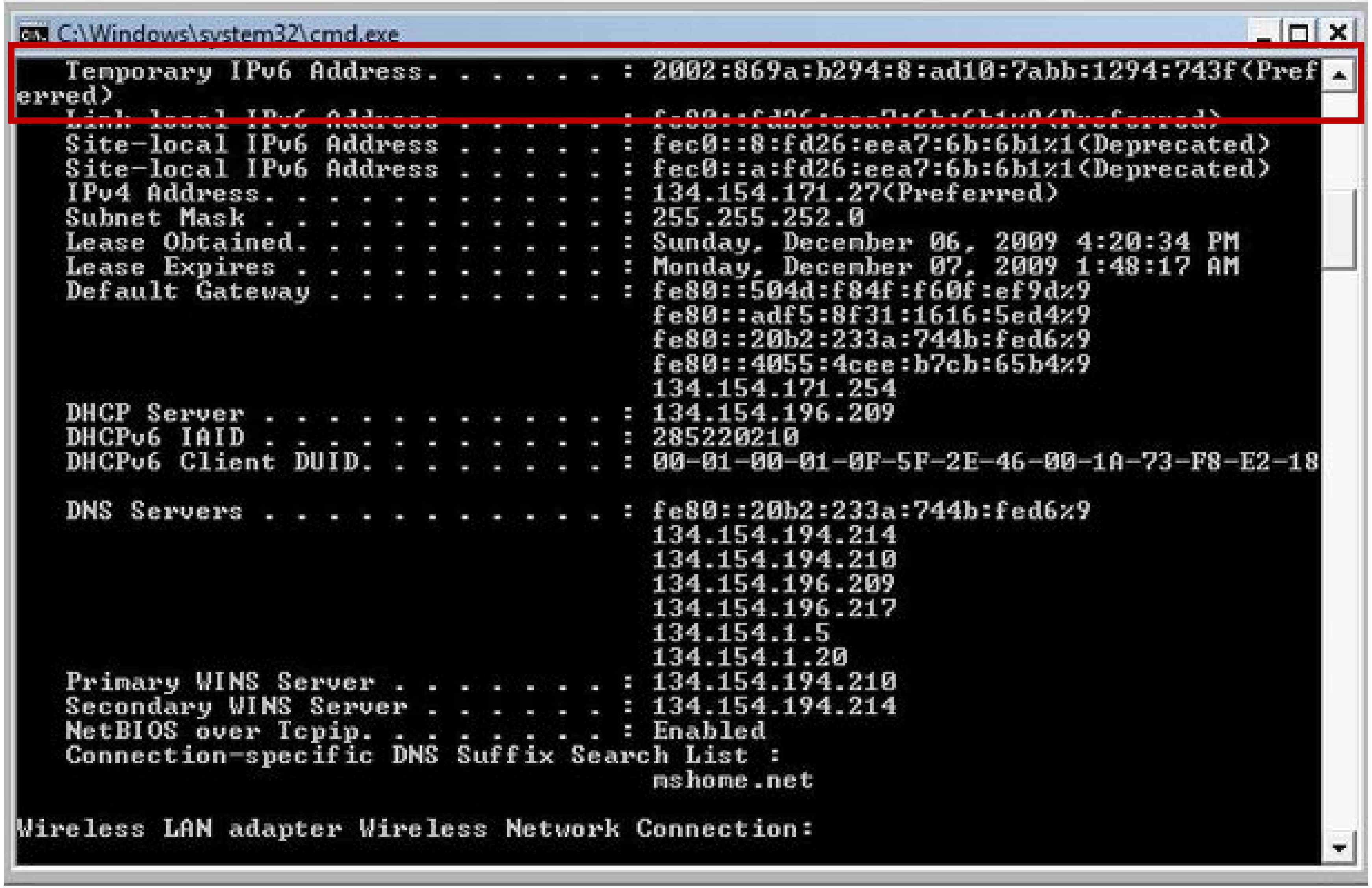
EUI-64 embeds your computer’s MAC address into the host portion of IPv6

- This means an adversary can recognize your PC and track your browsing activity
- It also means that you can be identified and tracked anywhere in the world
  - Your client address will always be the same, so your location can be tracked
    - All that’s needed is a known address you consistently visit no matter where you are

MITIGATIONS:

- This is why Windows and MacIntosh systems adopted RFC 4941 ‘Privacy Extensions’
  - Privacy Extensions for Stateless Address Autoconfiguration generates random host addresses
  - Windows and Mac hosts generate rotating additional ‘temporary’ addresses for outbound traffic
  - There is a known problem with generated values not being totally random, but it’s a good solution (if not a great one)
- Use DHCPv6 instead of SLAAC

IPv6 SCREEN CAPTURE



```
   Temporary IPv6 Address. . . . . . : 2002:869a:b294:8:ad10:7abb:1294:743f(Pref
erred)
   Link-local IPv6 Address . . . . . : fe80::fd26:eea7:6b:6b1%9(Preferred)
   Site-local IPv6 Address . . . . . : fec0::8:fd26:eea7:6b:6b1%1(Deprecated)
   Site-local IPv6 Address . . . . . : fec0::a:fd26:eea7:6b:6b1%1(Deprecated)
   IPv4 Address. . . . . . . . . . . : 134.154.171.27(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Lease Obtained. . . . . . . . . . : Sunday, December 06, 2009 4:20:34 PM
   Lease Expires . . . . . . . . . . : Monday, December 07, 2009 1:48:17 AM
   Default Gateway . . . . . . . . . : fe80::504d:f84f:f60f:ef9d%9
                                       fe80::adf5:8f31:1616:5ed4%9
                                       fe80::20b2:233a:744b:fed6%9
                                       fe80::4055:4cee:b7cb:65b4%9
                                       134.154.171.254
   DHCP Server . . . . . . . . . . . : 134.154.196.209
   DHCPv6 IAID . . . . . . . . . . . : 285220210
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-0F-5F-2E-46-00-1A-73-F8-E2-18

   DNS Servers . . . . . . . . . . . : fe80::20b2:233a:744b:fed6%9
                                       134.154.194.214
                                       134.154.194.210
                                       134.154.196.209
                                       134.154.196.217
                                       134.154.1.5
                                       134.154.1.20
   Primary WINS Server . . . . . . . : 134.154.194.210
   Secondary WINS Server . . . . . . : 134.154.194.214
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       mshome.net

Wireless LAN adapter Wireless Network Connection:
```

The vulnerability of unrecognized IPv6 traffic

Windows Vista and higher (both client and server systems) enable IPv6 by default

Macintosh Lion and higher systems enable IPv6 by default

Both OSes prefer IPv6 over IPv4

- Autoconfiguration will generate link-local addresses for all systems
  - The systems are reachable via IPv6 over Ethernet
    - This means host-to-host communication can occur without your knowledge
    - This means spoofed IPv6 gateways can be planted on your systems
      - The spoofed systems can run MITM attacks via a 6-to-4 proxy

MITIGATIONS:

- Run IPv6 security and detection tools even if you’re not actively using IPv6
- Disable IPv6 on your systems to lower your attack surface
- Migrate from a flat network to internal routed VLANs to create smaller local links

Manipulation of IPv6 DNS support

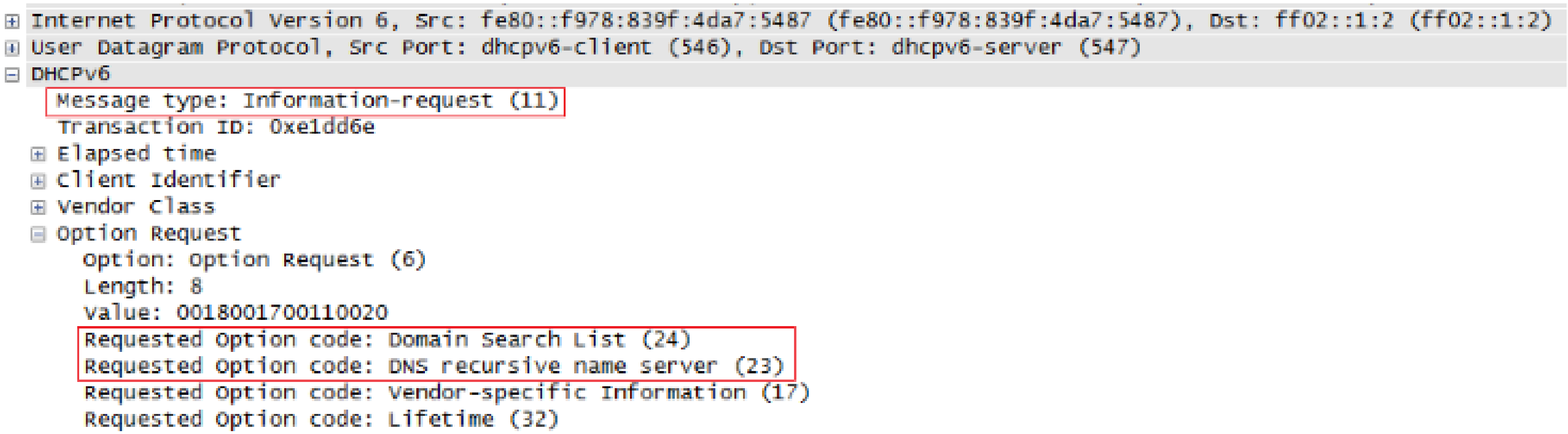
RFC 6106, “IPv6 Router Advertisement Options for DNS Configuration”, defines Recursive DNS Server (RDNSS) and DNS Search List (DNSSL) options for RAs

- These options (and also the Linux RDNSS daemon) leverage Network Discovery (ND) messages via FF02::FB, the All DNS servers multicast group)

MITIGATIONS:

- Specific to IPv6 is the monitoring and filtering of IPv6 DNS multicast ND packets.
- Autoconfiguration traffic (previously discussed) as another preventive measure.

DNSSEC would also expose false DNS servers



```
⊞ Internet Protocol Version 6, Src: fe80::f978:839f:4da7:5487 (fe80::f978:839f:4da7:5487), Dst: ff02::1:2 (ff02::1:2)
⊞ User Datagram Protocol, Src Port: dhcpv6-client (546), Dst Port: dhcpv6-server (547)
⊟ DHCPv6
    Message type: Information-request (11)
    Transaction ID: 0xe1dd6e
  ⊞ Elapsed time
  ⊞ Client Identifier
  ⊞ Vendor Class
  ⊟ Option Request
      Option: Option Request (6)
      Length: 8
      Value: 0018001700110020
      Requested Option code: Domain Search List (24)
      Requested Option code: DNS recursive name server (23)
      Requested Option code: Vendor-specific Information (17)
      Requested Option code: Lifetime (32)
```

ICMPv6 and the danger of spoofed “Neighbor” messages

Neighbor Discovery Protocol (RFC 2461) covers Neighbor Discovery ICMPv6 messages

- Some of the more vulnerable messages include
  - Type 134 – Router Advertisement (RA)
  - Type 135 – Neighbor Solicitation (NS)
  - Type 136 – Neighbor Advertisement (NA)
  - Type 137 – Route Redirection
- Most of these messages can be sent vis unicast or via multicast
- The messages are not signed or encrypted by default

Spoofed ICMPv6 RA messages in IPv6 environments

Since IPv6 RAs are not authenticated, spoofed RA messages are not detected by hosts

- This problem is documented in RFC 6104
- Spoofed RA messages can advertise
  - false gateways, DHCPv6-PD messages and router redirect messages
  - false autoconfiguration flags

MITIGATIONS:

- RFC 6104 solutions include
  - Manual configuration of IPv6 nodes
  - RA snooping controls (RFC 6105) and/or ACLs enabled on edge switches and host firewalls
    - But see RA Guard evasion (RFC 6980) for adversary evasion techniques
  - Layer 2 NAC and Layer 2 network partitioning

Spoofed Neighbor Solicitation messages

When a host automatically generates an IPv6 address (either link local or global), the host sends a NS message to the all-nodes multicast address (FF02::1)

- This is a Duplicate Address Detection (DAD) function to ensure unique addressing
  - Duplicate Address Detection (DAD) verifies an IPv6 address is unique before binding to the NIC
  - The DAD vulnerability is exploited when crafted response packets are delivered to the host running DAD, telling the host that each address it proffers is already in use
    - This will consume protocol resources, and could also totally exhaust available address options and leave the host unable to join the network
- A host could also spoof the role of another sytems (router, DHCP server, DNS server)

MITIGATION:

- Snoop Network Discovery traffic for excessive replies from one host.
- If available, place a limit or threshold on the maximum number of DAD responses that can be received from an edge port.

Spoofed Neighbor Advertisement messages

Similar to ARP Poisoning in IPv4

- The spoofed Neighbor Advertisement message lists all correct information about a neighbor, but substitutes the link-layer (MCA) address of a system involved in the attack (as in a MITM attack).

MITIGATION:

- Layer 2 edge switches should run IPv6 snooping to create tables between IPv6 address, ports, and link-layer (MAC) addresses.
  - Once a valid address has been obtained, the switch should reject any traffic not matching the host entry in the table.

IPv6 Route Redirection vulnerability

Redirect messages contain the link-layer address of the new first hop

- Useful in environments with multiple routers connected to the local subnet
- Router redirect messages are designed to inform a host of a better ‘next hop’
  - Spoofed router redirect messages can send traffic to malicious MITM routers
  - Spoofed router redirect messages can send traffic to non-existent routers
    - This creates a denial-of-service condition.

MITIGATION:

- Layer 2 edge switches should run IPv6 snooping to create tables between IPv6 address, ports, and link-layer (MAC) addresses.
  - Once a valid address has been obtained, the switch should reject any traffic not matching the host entry in the table.

ICMP Neighbor Discovery Security (RFC 3971)

Secure Neighbor Discovery (SeND) uses RSA key pairs to secure ICMP messages

- Each host generates a Cryptographically-Generated Address (CGA)
  - Found in the 64-bit Interface Identifier field
  - Permits host to verify the message came from the identified sender
  - Has built-in anti-replay functionality

- Summary on SeND
  - SeND is not widely supported, and without 100% adoption, networks are still vulnerable
  - SeND can’t check that a router is advertising its assigned addresses
  - SeND would require periodic maintenance of RSA keys on all designated hosts

Closing questions… (and my thanks!)