IPv6 is on my Network... But What Just Happened?!

Australian IPv6 Summit 2012

Jeffrey L Carrell

Network Conversions

Network Security Consultant
IPv6 SME/Trainer

Agenda

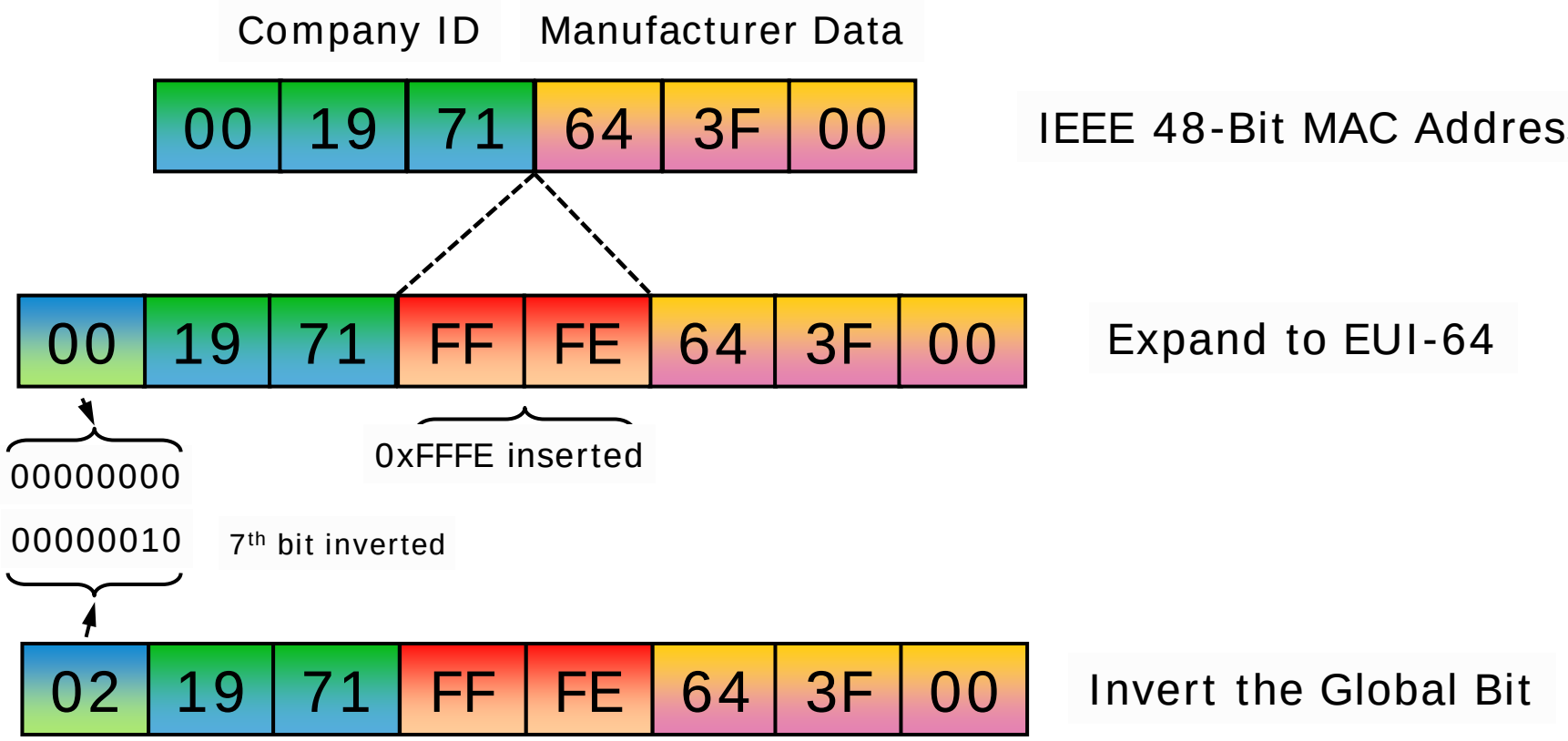
- IPv6 address fundamentals
- Operating Systems support
- ICMPv6 - Router Advertisement
- IPv6 address autoconfiguration
- IPv6 address autoconfiguration processes
- IPv6 address examples
- Security concerns
- System Demonstration

What is an IPv6 Address?

- IPv6 addresses are very different than IPv4 addresses in the size, numbering system, and delimiter between the numbers
  - 128bit -vs- 32bit
  - hexadecimal -vs- decimal
  - colon and double colon -vs- period (or “dot” for the real geeks)
- Valid IPv6 addresses are comprised of hexadecimal numbers (0-9 & a-f), with colons separating groups of four numbers, with a total of eight groups

  (each group is known as “quads”, “quartets”, or “chunks”)
  - 2001:0db8:1010:61ab:f005:ba11:00da:11a5
  - 2001:0000:0000:0A52:0000:0000:0000:3D16

Interface ID from MAC



Switch/Router operating systems

- May require software upgrade
- Generally disabled by default
- Generally uses M-EUI-64 Interface address
- May have client DHCPv6 support
- Generally no IPv6 “Temporary address” configured
- Generally support DHCPv6 relay on router interface
- May have DHCPv6 server
- If using IPv6 static routes, must use Link-Local addresses for next hop for ICMPv6 Redirect to work

Server operating systems

- Microsoft Server
  - 2003
    - Must be manually installed
    - Uses M-EUI-64 Interface address, no client DHCPv6 support
    - CLI configuration only
    - Limited server application support
      - no: AD, DHCPv6, RDP, Exchange, SQL, ftp
  - 2008/2012
    - Enabled by default
    - RFC 4941 privacy Interface addresses by default
      - No IPv6 “Temporary address” configured
    - GUI or CLI configuration
    - Most (if not all) server applications support IPv6
- Linux
  - Longest support, generally most server applications

Client operating systems

- Microsoft Windows
  - XP – w/SP2 - must install IPv6 protocol
    - Uses M-EUI-64 Interface address, no client DHCPv6 support
    - CLI configuration only
  - Vista, 7, 8 - enabled by default
    - RFC 4941 privacy Interface addresses by default
    - GUI and CLI configuration
- Apple Mac OS X
  - Mac OS X 10.4+ - native and enabled by default
    - Uses M-EUI-64 Interface address by default, no client DHCPv6 support ** DHCPv6 support in Lion !!!!!!
    - GUI and CLI configuration
- Linux
  - Generally enabled by default

Network peripherals

- Printers
- VoIP phones
- Network cameras
- Embedded systems

** More manufacturers are supporting IPv6 in their devices

*** and IPv6 ready or supported does not mean the same thing to everybody!!!

ICMPv6 - Router Advertisement

- Router Advertisement (RA) [key components]
  - M flag – managed address configuration flag
    (stateful (DHCPv6) autoconfig)
  - O flag – other configuration flag
    (stateless DHCPv6 autoconfig)
  - Router Lifetime – lifetime associated with the default router
  - Prefix Length – number of bits in the prefix
  - A flag – autonomous address-configuration flag
  - L flag – on-link flag
  - Valid Lifetime – length of time the address is valid for use in preferred and deprecated states
  - Preferred Lifetime – length of time the address is valid for new communications
  - Prefix – IPv6 address prefix

– **For additional info, see RFC 4861**

IPv6 autoconfiguration options

Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags M Flag	ICMPv6 RA (Type 134) Flags O Flag	ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info A Flag	ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info L Flag	Prefix Derived from	Interface ID Derived from	Other Configuration Options
Link-Local (always configured)	N/A	N/A	N/A	N/A	Internal (fe80::)	M-EUI-64 or Privacy	Manual
SLAAC	Off	Off	On	On	RA	M-EUI-64 or Privacy	Manual
Stateful (DHCPv6)	On	On	Off	On	DHCPv6	DHCPv6	DHCPv6
Stateless DHCPv6	Off	On	On	On	RA	M-EUI-64 or Privacy	DHCPv6
Combination Stateless & DHCPv6 (results in up to 3 IPv6 addresses per network prefix)	On	On	On	On	RA and DHCPv6	M-EUI-64 or Privacy and DHCPv6	DHCPv6

Router Advertisement packet

```
Frame 691: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)
Ethernet II, Src: Procurve_db:1d:00 (00:1b:3f:db:1d:00), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::21b:3fff:fedb:1d00 (fe80::21b:3fff:fedb:1d00), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0xd709 [correct]
  Cur hop limit: 64
  Flags: 0xc0
    1... .... = Managed address configuration: 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
  Reachable time (ms): 0
  Retrans timer (ms): 0
  ICMPv6 Option (Source link-layer address : 00:1b:3f:db:1d:00)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: Procurve_db:1d:00 (00:1b:3f:db:1d:00)
  ICMPv6 Option (Prefix information : 2001:db8:1ab:1::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
    Flag: 0xc0
      1... .... = On-link flag(L): Set
      .1.. .... = Autonomous address-configuration flag(A): Set
      ..00 0000 = Reserved: 0
    Valid Lifetime: 40
    Preferred Lifetime: 20
    Reserved
    Prefix: 2001:db8:1ab:1:: (2001:db8:1ab:1::)
  ICMPv6 Option (Prefix information : 2001:db8:1ab:ba5e::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
    Flag: 0xc0
      1... .... = On-link flag(L): Set
      .1.. .... = Autonomous address-configuration flag(A): Set
      ..00 0000 = Reserved: 0
    Valid Lifetime: 40
    Preferred Lifetime: 20
    Reserved
    Prefix: 2001:db8:1ab:ba5e:: (2001:db8:1ab:ba5e::)
```

Router Advertisement packet

```
Frame 691: 142 bytes on wire (1136 bits), 142 bytes captured (1136 b
Ethernet II, Src: Procurve_db:1d:00 (00:1b:3f:db:1d:00), Dst: IPv6mc
Internet Protocol Version 6, Src: fe80::21b:3fff:fedb:1d00 (fe80::21
Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xd709 [correct]
    Cur hop limit: 64
  Flags: 0xc0
      1... .... = Managed address configuration: 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
    Reachable time (ms): 0
    Retrans timer (ms): 0
```

Router Advertisement packet

```
ICMPv6 Option (Prefix information : 2001:db8:1ab:1::/64)
  Type: Prefix information (3)
  Length: 4 (32 bytes)
  Prefix Length: 64
⊟ Flag: 0xc0
    1... .... = On-link flag(L): Set
    .1.. .... = Autonomous address-configuration flag(A): Set
    ..00 0000 = Reserved: 0
  Valid Lifetime: 40
  Preferred Lifetime: 20
  Reserved
  Prefix: 2001:db8:1ab:1:: (2001:db8:1ab:1::)
ICMPv6 Option (Prefix information : 2001:db8:1ab:ba5e::/64)
  Type: Prefix information (3)
  Length: 4 (32 bytes)
  Prefix Length: 64
⊟ Flag: 0xc0
    1... .... = On-link flag(L): Set
    .1.. .... = Autonomous address-configuration flag(A): Set
    ..00 0000 = Reserved: 0
  Valid Lifetime: 40
  Preferred Lifetime: 20
  Reserved
  Prefix: 2001:db8:1ab:ba5e:: (2001:db8:1ab:ba5e::)
```

IPv6 address autoconfiguration

- Assigning an IPv6 address:
  - Link-Local (automatically assigned when IPv6 is enabled)
    - Based on prefix FE80::/64
    - Interface ID (64 bit host portion) derived from either:
      - Modified IEEE EUI-64 format (RFC 4291)
        - Derived from MAC address
      - Privacy format (RFC 4941)
        - Derived from random number generator

❖NOTE: Requires no routers, no DHCPv6 servers, no additional network systems support.

IPv6 address autoconfiguration, con't

- Assigning an IPv6 address:
  - Autoconfiguration
    - SLAAC (Stateless address autoconfiguration), generally a /64
      - Uses prefix information from Router Advertisement
      - Interface ID (64 bit host portion) derived from either:
        - Modified IEEE EUI-64 format (RFC 4291)
          - Derived from MAC address
        - Privacy format (RFC 4941)
          - Derived from random number generator
          - Generally creates 2 global addresses
        - Cryptographically generated (RFC 3972)
          - Secure/unique interface ID
    - Stateful
      - generally via DHCPv6 (RFC 3315)

con't -->

IPv6 address autoconfiguration, con't

- Assigning an IPv6 address:
  - Autoconfiguration, con't
    - Stateless DHCPv6
      - Uses prefix information from Router Advertisement
      - Interface ID (64 bit host portion) derived from either:
        - Modified IEEE EUI-64 format (RFC 4291)
          - Derived from MAC address
        - Privacy format (RFC 4941)
          - Derived from random number generator
        - Cryptographically generated (RFC 3972)
          - Secure/unique interface ID
      - Uses DHCPv6 for "other" information
        - DNS, etc

IPv6 SLAAC process

- A node sends a multicast Router Solicitation message to the “all-routers” address FF02::2
- Router(s) respond with Router Advertisement message containing prefix(es) for stateless autoconfiguration
- The node configures its own IPv6 address(es) with the advertised prefix(es), plus a locally-generated Interface ID
- Node checks whether the selected address(es) is(are) unique (Duplicate Address Detection)
- If unique, the address(es) is(are) configured on interface

IPv6 Stateful (DHCPv6) process

- A node sends a multicast Router Solicitation message to the “all-routers” address FF02::2
- Router(s) respond with Router Advertisement message containing M flag for stateful autoconfiguration
- The node sends a multicast Solicit message to the “all-DHCP relay agents and servers” address FF02::1:2
- DHCPv6 server(s) responds with Advertise message(s) containing IPv6 address and lifetimes
- The node sends a Request message to confirm and seeking other information
- DHCPv6 server responds with Reply message
- Node checks whether the selected address is unique (Duplicate Address Detection)
- If unique, the address is configured on interface

IPv6 Stateless DHCPv6 process

- A node sends a multicast Router Solicitation message to the “all-routers” address FF02::2
- Router(s) respond with Router Advertisement message containing prefix(es) and O flag for stateless DHCPv6 autoconfiguration
- The node configures its own IPv6 address(es) with the advertised prefix(es), plus a locally-generated Interface ID
- The node sends a multicast Information-Request message to the “all-DHCP relay agents and servers” address FF02::1:2
- DHCPv6 server responds with Reply message
- Node checks whether the selected address is unique (Duplicate Address Detection)
- If unique, the address is configured on interface

Key difference in DHCP/DHCPv6

- Default gateway
  - DHCP – configurable Router option in scope
  - DHCPv6 – no configurable Router option in scope

- An IPv6 node derives its default gateway from the router's Link-Local address when the L flag is set in the Prefix information field of an RA
  (! not from the network prefix !)

IPv6 addresses on Win7 client

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : ipv6sandbox.com
   Description . . . . . . . . . . . : ASIX AX88772A USB2.0 to Fast Ethernet Adapter
   Physical Address. . . . . . . . . : 00-60-6E-61-10-F7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:1ab:1:4805:44e:b663:6c1e(Preferred)
   IPv6 Address. . . . . . . . . . . : 2001:db8:1ab:ba5e::100(Preferred)
   Lease Obtained. . . . . . . . . . : Wednesday, April 04, 2012 4:00:40 PM
   Lease Expires . . . . . . . . . . : Thursday, April 05, 2012 3:56:21 PM
   IPv6 Address. . . . . . . . . . . : 2001:db8:1ab:ba5e:4805:44e:b663:6c1e(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:db8:1ab:1:db1:1341:34b5:7bf8(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:db8:1ab:ba5e:db1:1341:34b5:7bf8(Preferred)
   Link-local IPv6 Address . . . . . : fe80::4805:44e:b663:6c1e%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.1.0.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, April 04, 2012 4:00:27 PM
   Lease Expires . . . . . . . . . . : Thursday, April 05, 2012 3:56:08 PM
   Default Gateway . . . . . . . . . : fe80::21b:3fff:fedb:1d00%17
                                       10.1.0.1
   DHCP Server . . . . . . . . . . . : 10.1.0.200
   DHCPv6 IAID . . . . . . . . . . . : 402677870
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-15-88-94-DE-E0-2A-82-3A-A7-5D
   DNS Servers . . . . . . . . . . . : 2001:db8:1ab:ba5e::2000
                                       10.1.0.200
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       ipv6sandbox.com
```

IPv6 addresses on Mac Lion client

```
nb19:~ jcarrell$ ifconfig -L en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=2b<RXCSUM,TXCSUM,VLAN_HWTAGGING,TSO4>
        ether c8:bc:c8:a0:16:93
        inet6 fe80::cabc:c8ff:fea0:1693%en0 prefixlen 64 scopeid 0x4
        inet 169.254.161.176 netmask 0xffff0000 broadcast 169.254.255.255
        inet6 2001:db8:1ab:ba5e:cabc:c8ff:fea0:1693 prefixlen 64 autoconf pltime 17 vltime 37
        inet6 2001:db8:1ab:ba5e:7d55:93db:ba82:859a prefixlen 64 autoconf temporary pltime 17 vltime 37
        inet6 2001:db8:1ab:ba5e::102 prefixlen 64 tentative pltime 58 vltime 118
        media: autoselect (1000baseT <full-duplex>)
        status: active
nb19:~ jcarrell$ netstat -nr |grep default
default            link#4             UCS              2        0     en0
default                                 fe80::216:35ff:feb3:76c0%en0    UGc             en0
nb19:~ jcarrell$ cat /etc/resolv.conf
#
# Mac OS X Notice
#
# This file is not used by the host name and address resolution
# or the DNS query routing mechanisms used by most processes on
# this Mac OS X system.
#
# This file is automatically generated.
#
search ipv6sandbox.com
nameserver 2001:db8:1ab:ba5e::2000
```

Security concerns

- If EUI-64 based address, can determine manufacturer of interface, which may lead to what type of device it is, and where in the network in may be located.
- Since IPv6 is enabled by default in many operating systems and devices, simple scan of network will provide tons of info
- Many “tools” already available for exploitation of devices/systems
- Easy to spoof clients with rogue RA (use RA Guard on switches to block RAs on non-trusted interfaces)
- If there is a “Temporary” IPv6 address in addition to a regular RA configured IPv6 address, the “Temporary” address is used for outbound communications by the client. “Temporary” IPv6 addresses can change frequently.

HP switch - IPv6 VLAN config

```
vlan 1
    ip address 10.1.0.1 255.255.255.0
    ipv6 enable
    ipv6 address 2001:db8:1ab:ba5e::1/64
    ipv6 nd ra managed-config-flag
    ipv6 nd ra other-config-flag
    ipv6 nd ra max-interval 130
    ipv6 nd ra min-interval 30
    ipv6 nd ra prefix 2001:db8:1ab:1::/64 40 20
    ipv6 nd ra prefix 2001:db8:1ab:ba5e::/64 40 20
```

Cisco switch - IPv6 VLAN config

```
interface Vlan1
 ip address 10.1.0.2 255.255.255.0
 ipv6 address 2001:DB8:1AB:BA5E::2/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1AB:BA5E::/64 30 10
 ipv6 nd other-config-flag
 ipv6 nd ra interval 40 15
end
```

Router Advertisement packet (good)

```
No.     Time        Source                Destination           Protocol Length Info
   1282 12:18:21    fe80::20c:29ff:fe35:e8c1 ff02::1               ICMPv6   110 Router Advertisement
```

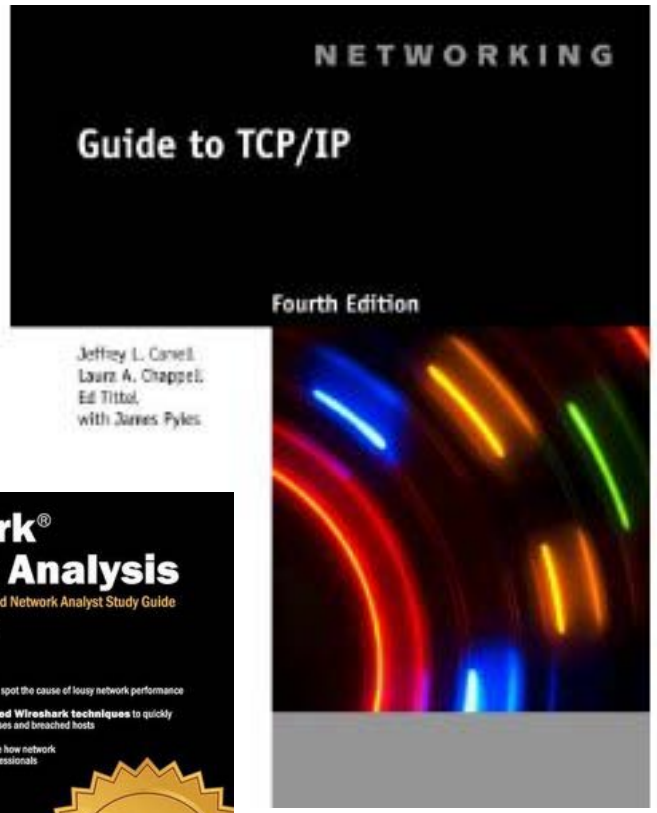
```
⊞ Frame 1282: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
⊞ Ethernet II, Src: Vmware_35:e8:c1 (00:0c:29:35:e8:c1), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
⊞ Internet Protocol Version 6, Src: fe80::20c:29ff:fe35:e8c1 (fe80::20c:29ff:fe35:e8c1), Dst: ff02::1 (ff(
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xe3c1 [correct]
    Cur hop limit: 64
  ⊟ Flags: 0xc0
      1... .... = Managed address configuration: 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): 540
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ⊟ ICMPv6 Option (Prefix information : 2001:db8:1ab:ba5e::/64)
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
    ⊟ Flag: 0x80
        1... .... = On-link flag(L): Set
        .0.. .... = Autonomous address-configuration flag(A): Not set
        ..0. .... = Router address flag(R): Not set
        ...0 0000 = Reserved: 0
      Valid Lifetime: 300
      Preferred Lifetime: 240
      Reserved
      Prefix: 2001:db8:1ab:ba5e:: (2001:db8:1ab:ba5e::)
  ⊟ ICMPv6 Option (Source link-layer address : 00:0c:29:35:e8:c1)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: Vmware_35:e8:c1 (00:0c:29:35:e8:c1)
```

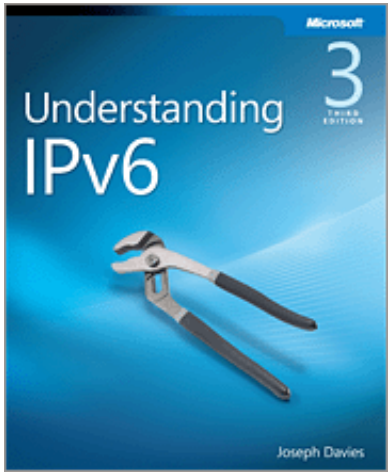
Router Advertisement packet (bad)

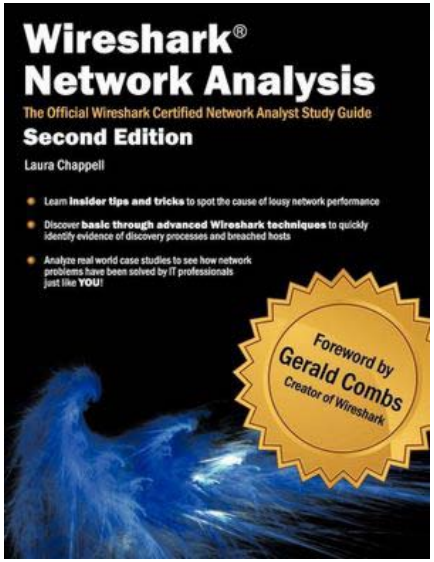
```
No.     Time        Source                Destination           Protocol Length Info
   1289 12:18:51    fe80::20c:29ff:fee8:b4b4 ff02::1               ICMPv6    110 Router Advertisement

⊞ Frame 1289: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
⊞ Ethernet II, Src: Vmware_e8:b4:b4 (00:0c:29:e8:b4:b4), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
⊞ Internet Protocol Version 6, Src: fe80::20c:29ff:fee8:b4b4 (fe80::20c:29ff:fee8:b4b4), Dst: ff02::1 (ff(
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x8d20 [correct]
    Cur hop limit: 64
  ⊟ Flags: 0x48
      0... .... = Managed address configuration: Not set
      .1.. .... = Other configuration: Set
      ..0. .... = Home Agent: Not set
      ...0 1... = Prf (Default Router Preference): High (1)
      .... .0.. = Proxy: Not set
      .... ..0. = Reserved: 0
    Router lifetime (s): 777
    Reachable time (ms): 0
    Retrans timer (ms): 0
  ⊟ ICMPv6 Option (Prefix information : 2001:db8:1ab:7777::/64)
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
    ⊟ Flag: 0xc0
        1... .... = On-link flag(L): Set
        .1.. .... = Autonomous address-configuration flag(A): Set
        ..0. .... = Router address flag(R): Not set
        ...0 0000 = Reserved: 0
      Valid Lifetime: 300
      Preferred Lifetime: 120
      Reserved
      Prefix: 2001:db8:1ab:7777:: (2001:db8:1ab:7777::)
  ⊟ ICMPv6 Option (Source link-layer address : 00:0c:29:e8:b4:b4)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: Vmware_e8:b4:b4 (00:0c:29:e8:b4:b4)
```

Resources

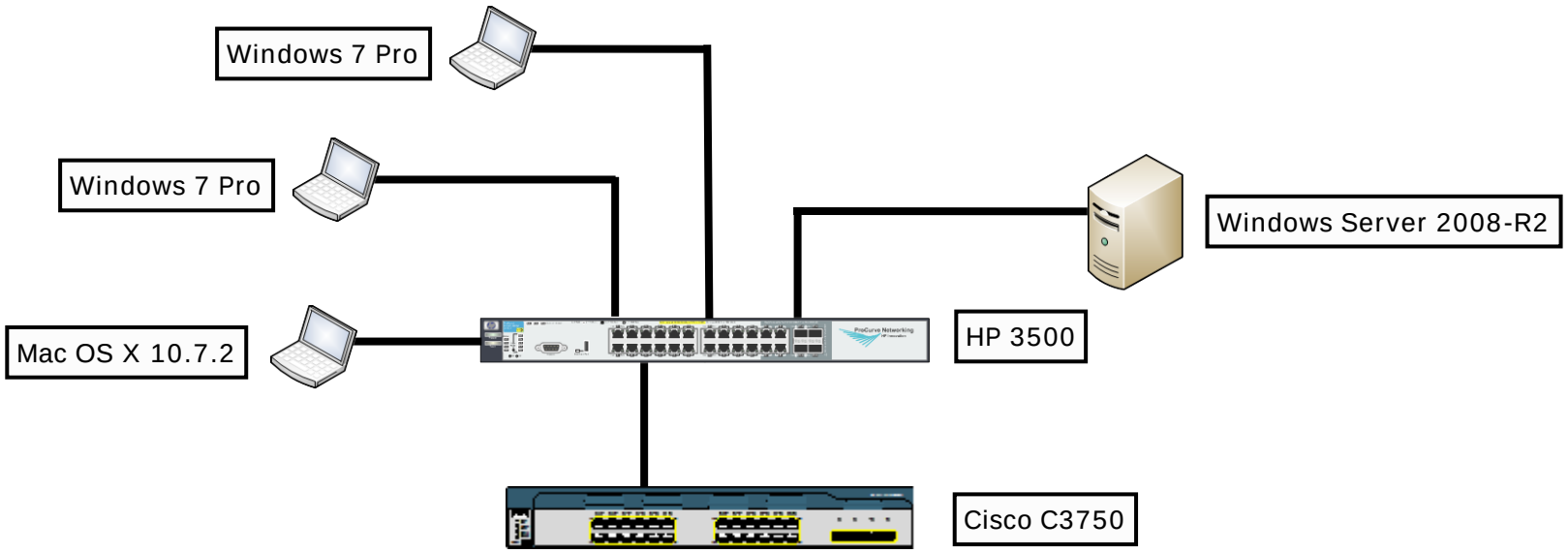
- Guide to TCP/IP, 4th Edition
  (Published September 2012)
- Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide
  (Published March 2012)
- Understanding IPv6, 3rd Edition
  (Published June 2012)







System demonstration



Questions ??????

Thank You for Attending!

Jeffrey L Carrell

Network Security Consultant

jeff.carrell@networkconversions.com