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

2012 North American IPv6 Summit

Jeffrey L Carrell

Network Conversions

Network Security Consultant

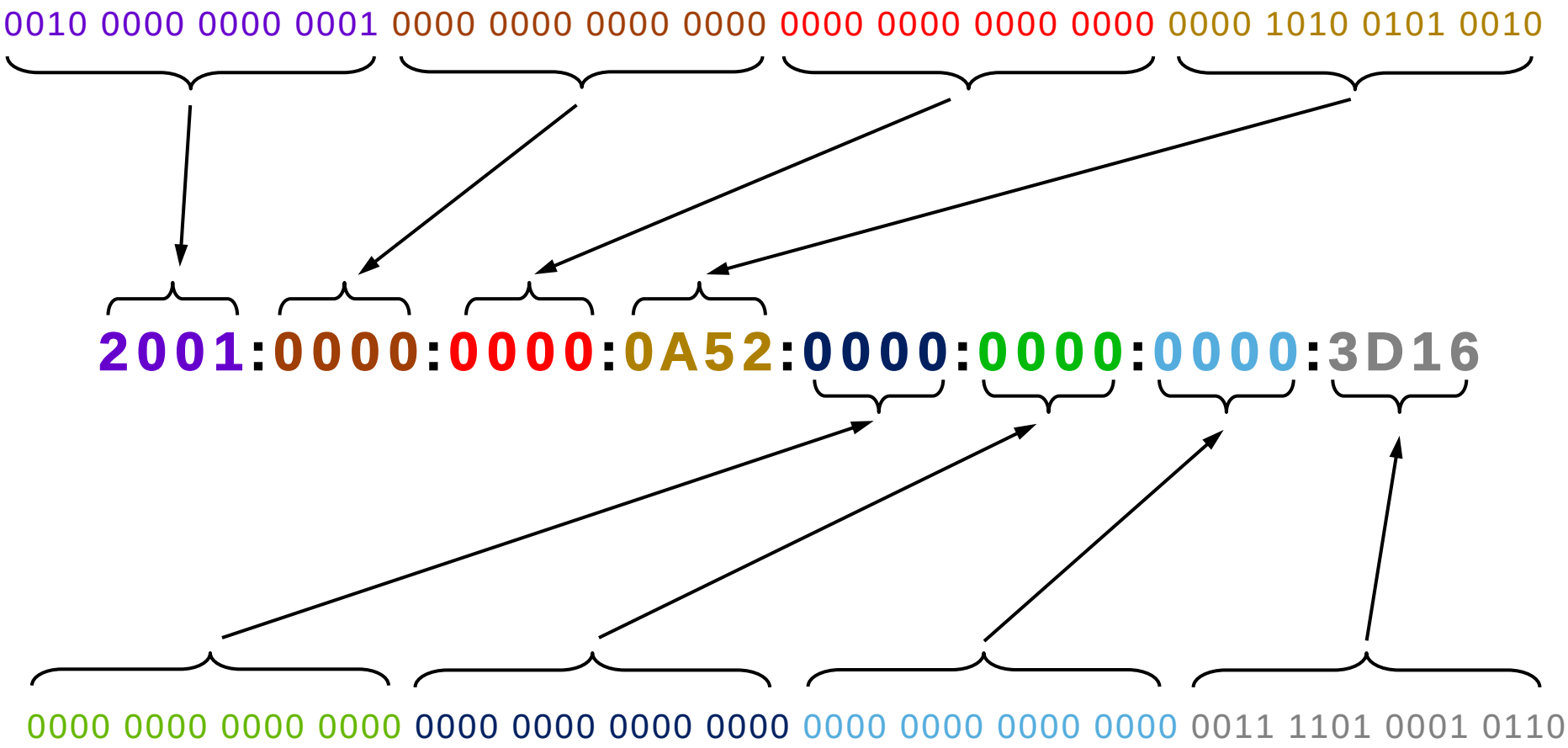
Agenda

- IPv6 address fundamentals
- IPv6 address autoconfiguration
- Router Advertisement
- IPv6 address autoconfiguration operations
- Switch/Router operating systems
- Server operating systems
- Client operating systems
- Security concerns
- System Demonstration

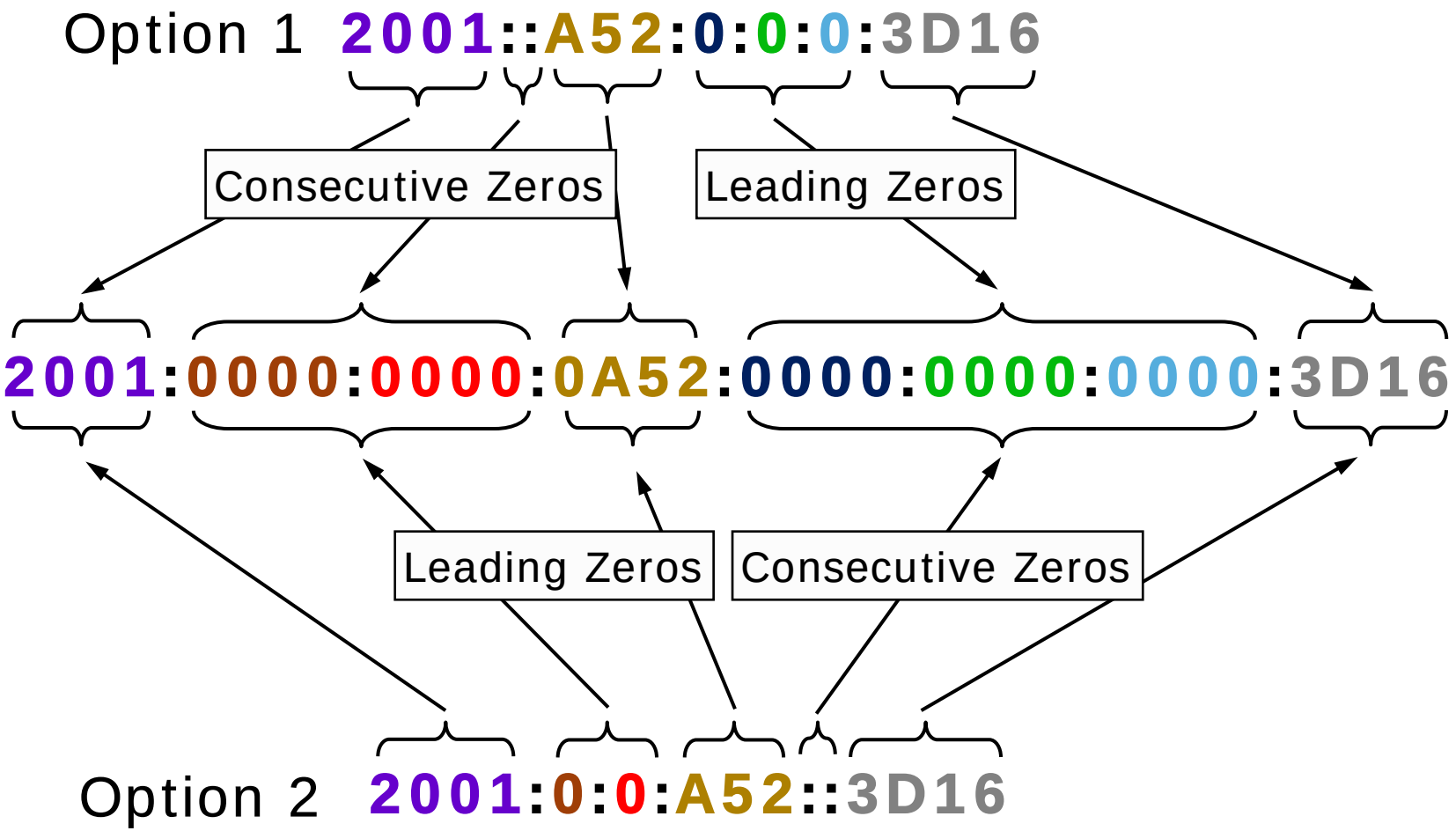
Remember -----

- What network protocols you were running in 1990 ?
  - IPX/SPX – Novell
  - AppleTalk – Apple
  - NetBIOS/NetBEUI – Sytek, IBM, Microsoft
  - DECnet – DEC
  - XNS – Xerox
  - Others ???
- What network protocols you were running in 2000 ?
  - IP (IPv4)
  - IPv6 maybe ??
- How many of you were involved in the conversion of one or more of these protocols to IP (IPv4)?

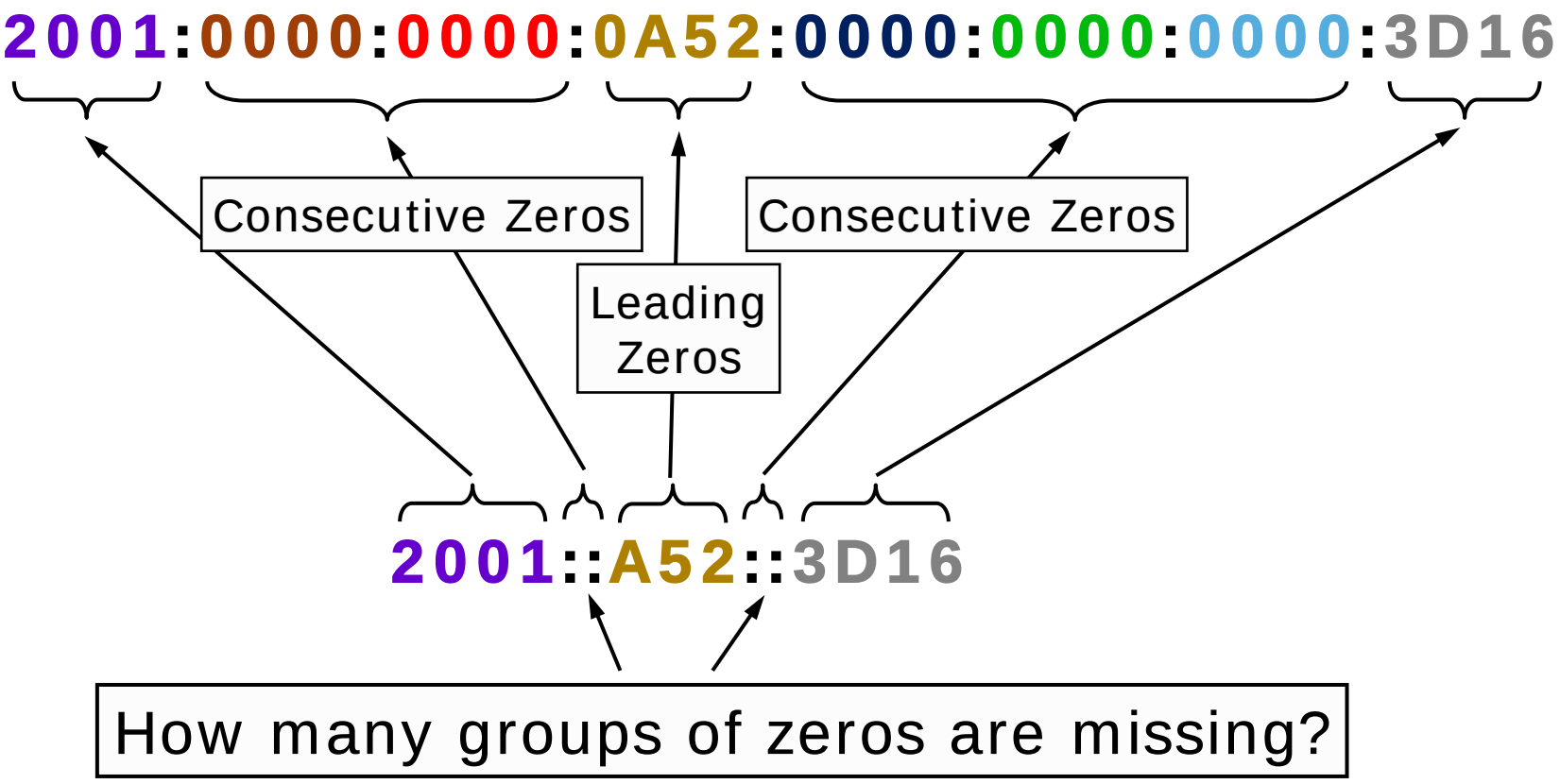
Hexadecimal notation



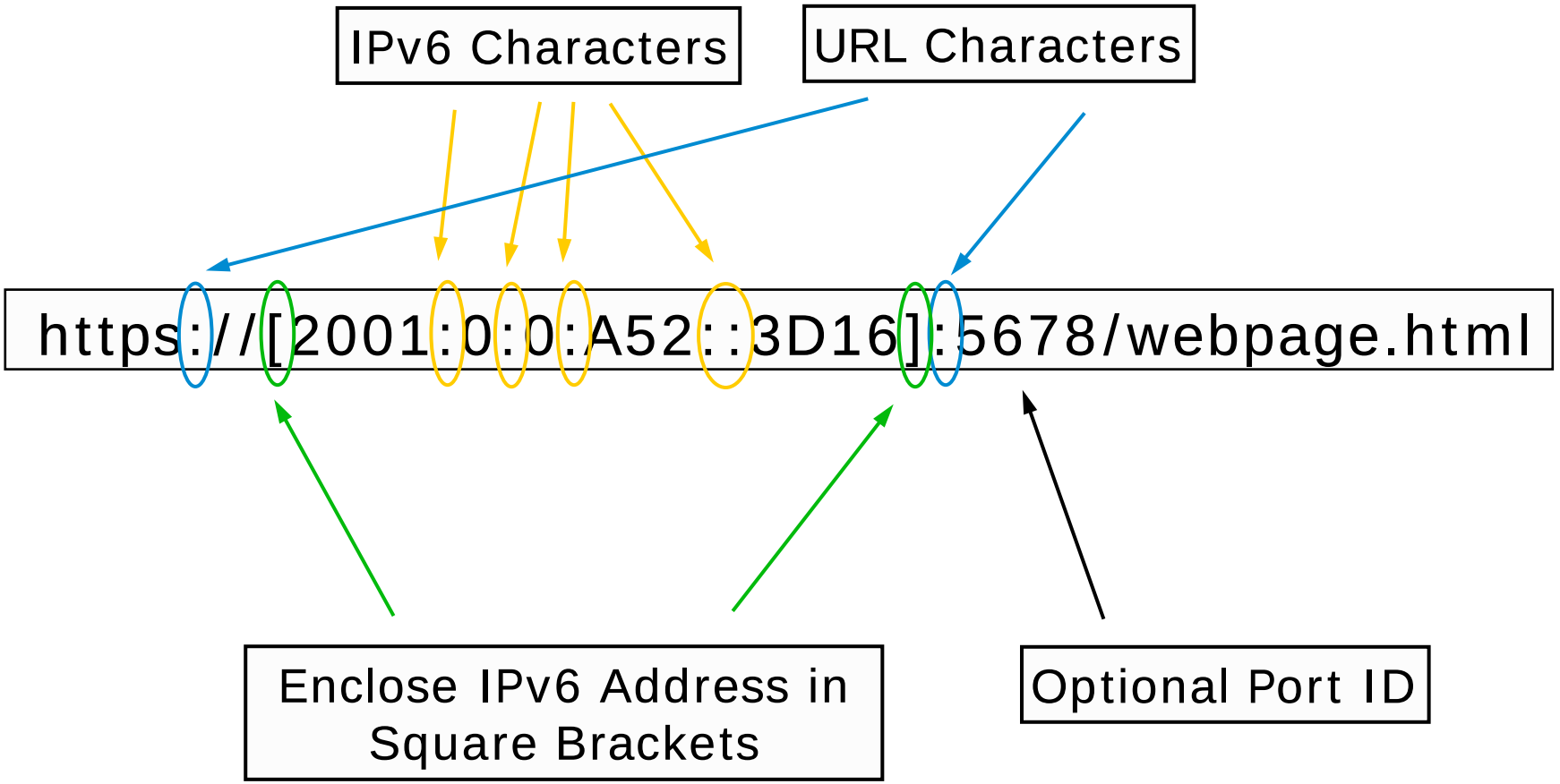
IPv6 shorthand notation



Incorrect shorthand notation



Mixed URL & IPv6 notation in URL



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

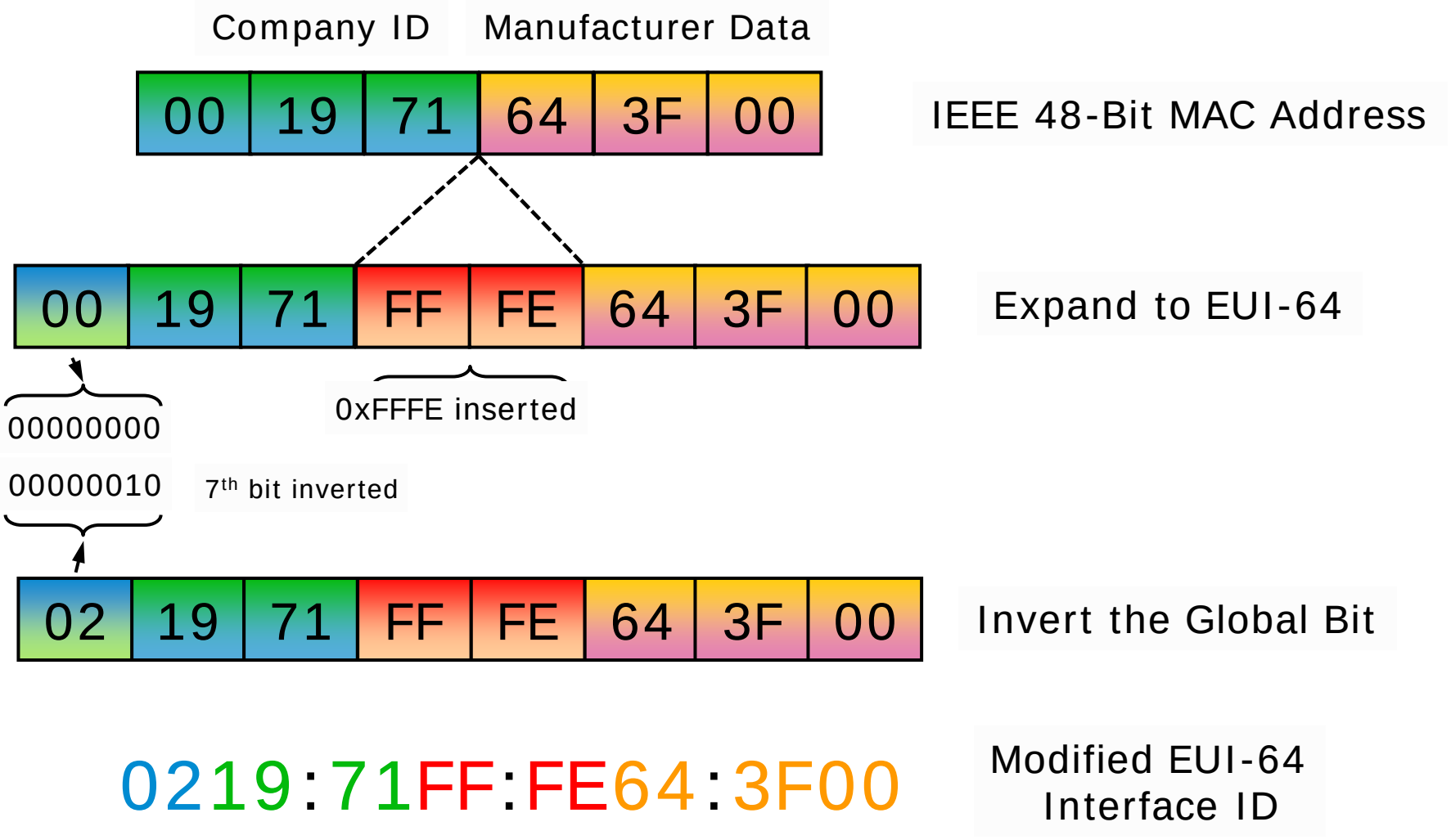
- Assigning an IPv6 address:
  - Autoconfiguration
    - SLAAC (Stateless address autoconfiguration), generally a /64
      - Uses prefix information from Router Advertisement
      - Interface ID (64 bit host portion) derived from either:
        - Modified IEEE EUI-64 format (RFC 4291)
          - Derived from MAC address
        - Privacy format (RFC 4941)
          - Derived from random number generator
        - 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

Interface ID from MAC



Router Advertisement

- Router Advertisement (RA) [key components]
  - M flag – managed address configuration flag (stateful autoconfig)
  - O flag – other configuration flag
  - 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 prefix is valid
  - Preferred Lifetime – length of time the address (generated from the prefix) is valid
  - Prefix – IPv6 address prefix

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

IPv6 autoconfiguration options

Address Autoconfiguration Method	RA ICMPv6 Field M Flag	RA ICMPv6 Field O Flag	RA ICMPv6 Prefix Info Option A Flag	RA ICMPv6 Prefix Info Option L Flag	Prefix Derived from	Interface ID Derived from	Other Configuration Options
Link-Local	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 3 [or more] IPv6 addresses)	On	On	On	On	RA and DHCPv6	M-EUI-64 or Privacy and DHCPv6	DHCPv6

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 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

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
    - Enabled by default
    - RFC3041 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
    - RFC3041 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

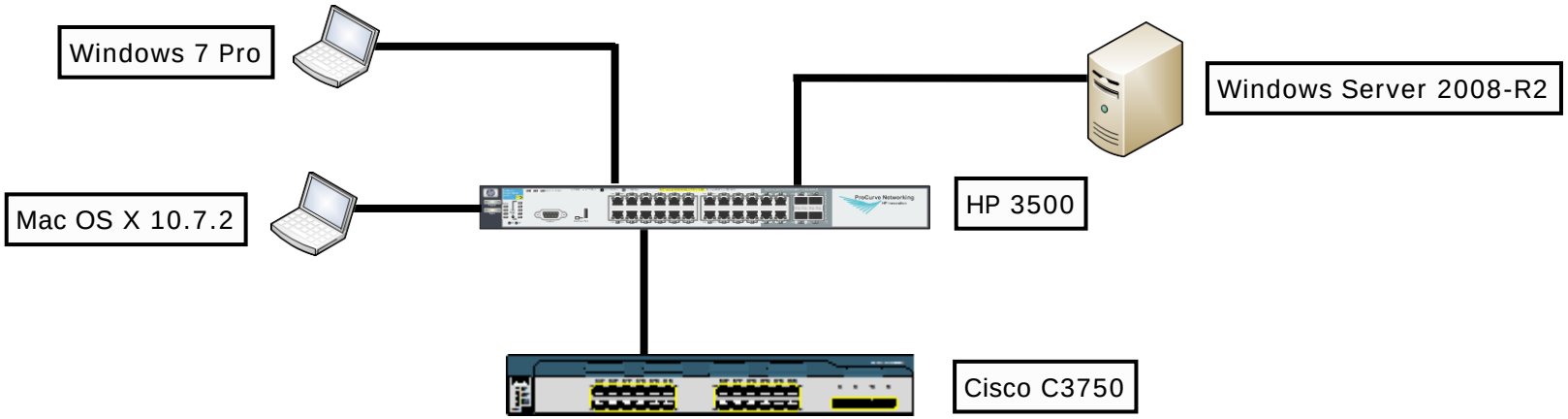
** More manufacturers are supporting IPv6 in their devices

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

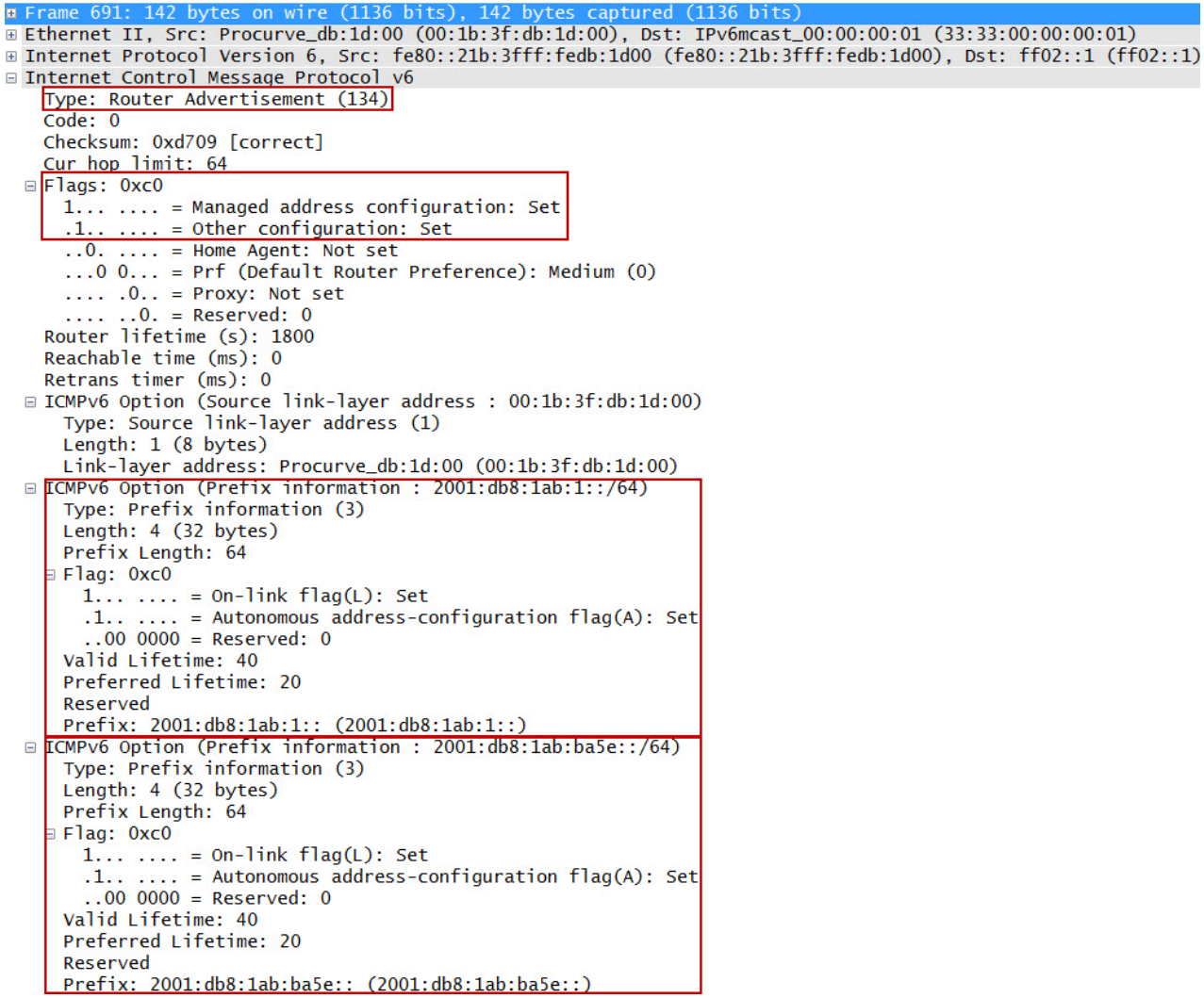
Security concerns

- 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.

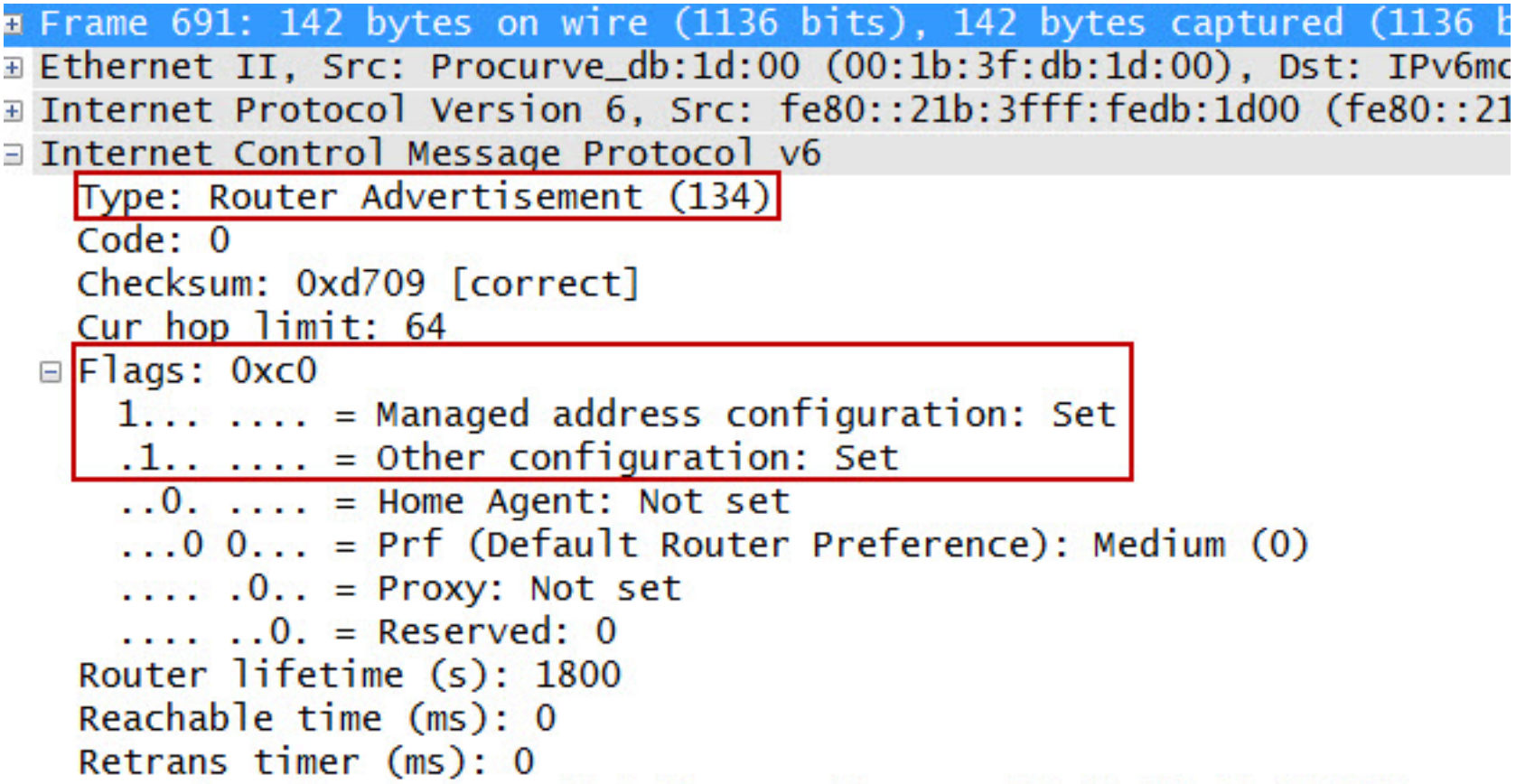
System demonstration



Router Advertisement packet



Router Advertisement packet



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 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
```

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
```

Microsoft IPv6 forum post

I am using DHCPv6 in my local LAN to configure IPv6 on to my client machines (windows) and gateway using router by using M bit 1 in RA. Everything is fine up to that. Whenever I run an script to send rogue RA into my LAN, client machines configure the ipv6 addresses according to that RA but remove IPv6 address taken from DHCPv6. I am bit surprised why the client (windows 7) removing IPv6 address taken from DHCPv6 from it stack. It should keep both the IPs as I could see both the gateways on client.
Secondly, Now I am running another script to kill that forge RA by sending RA with 0 lifetime to that prefix (with same source). In that case RA has been killed as interface unassigned that gateway but still client machine don't put IPv6 address on its interface provided by DHCPv6.
This shows Client machine prefers RA over DHCPv6.

Thank You for Attending!

Jeffrey L Carrell

Network Security Consultant

jeff.carrell@networkconversions.com

jeff.carrell@ipv6hol.com