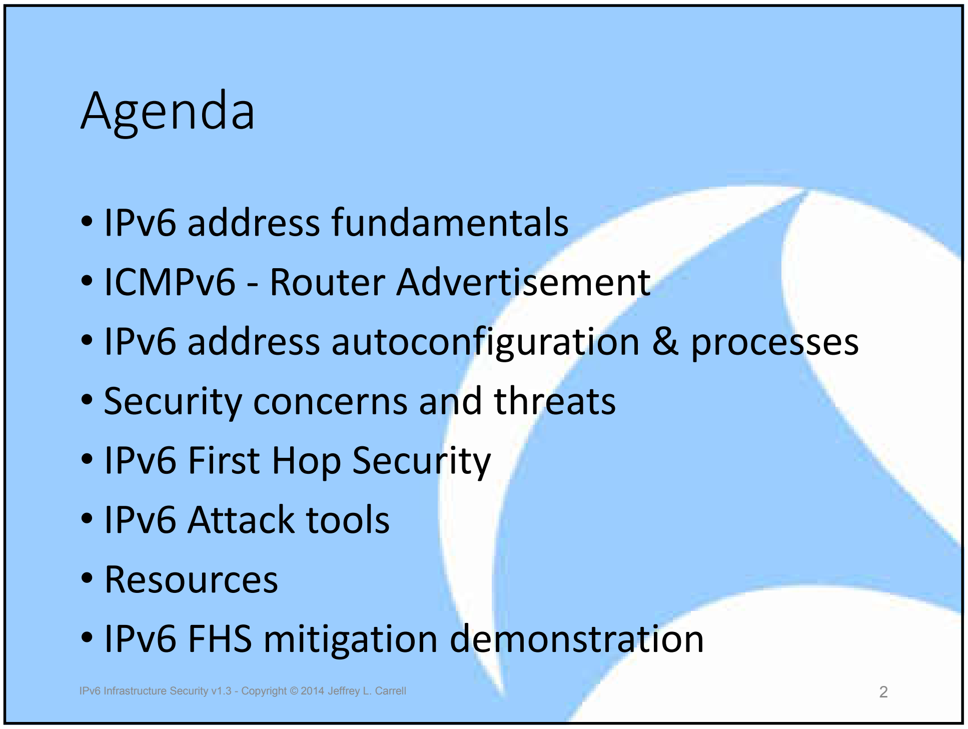
SHARKFEST '14
WIRESHARK DEVELOPER AND USER CONFERENCE
JUNE 16-20 2014 · DOMINICAN UNIVERSITY

IPv6 Infrastructure Security

Jeffrey L Carrell
Network Security Consultant , IPv6 SME/Trainer
jeff.carrell@teachmeipv6.com
jeff.carrell@networkconversions.com
@JeffCarrell_v6

IPv6 FORUM CERTIFIED ENGINEER
IPv6 FORUM CERTIFIED TRAINER
Certificate of Completion
jeffcarrell
Sage
Hurricane Electric IPv6 Certification

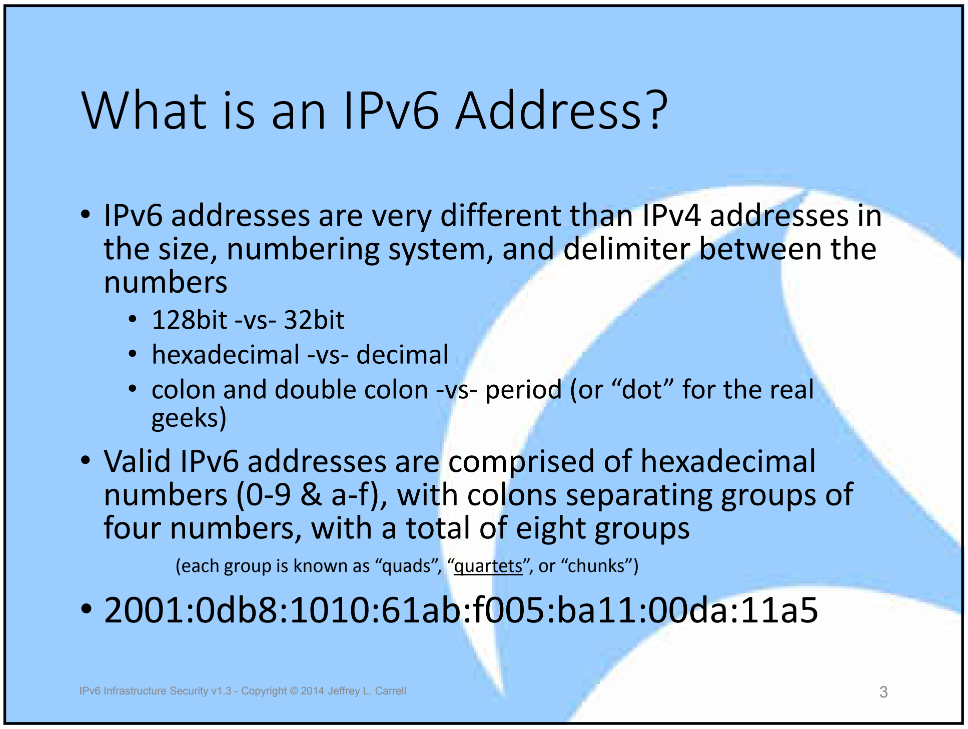
IPv6 Infrastructure Security v1.3



Agenda

- IPv6 address fundamentals
- ICMPv6 - Router Advertisement
- IPv6 address autoconfiguration & processes
- Security concerns and threats
- IPv6 First Hop Security
- IPv6 Attack tools
- Resources
- IPv6 FHS mitigation demonstration

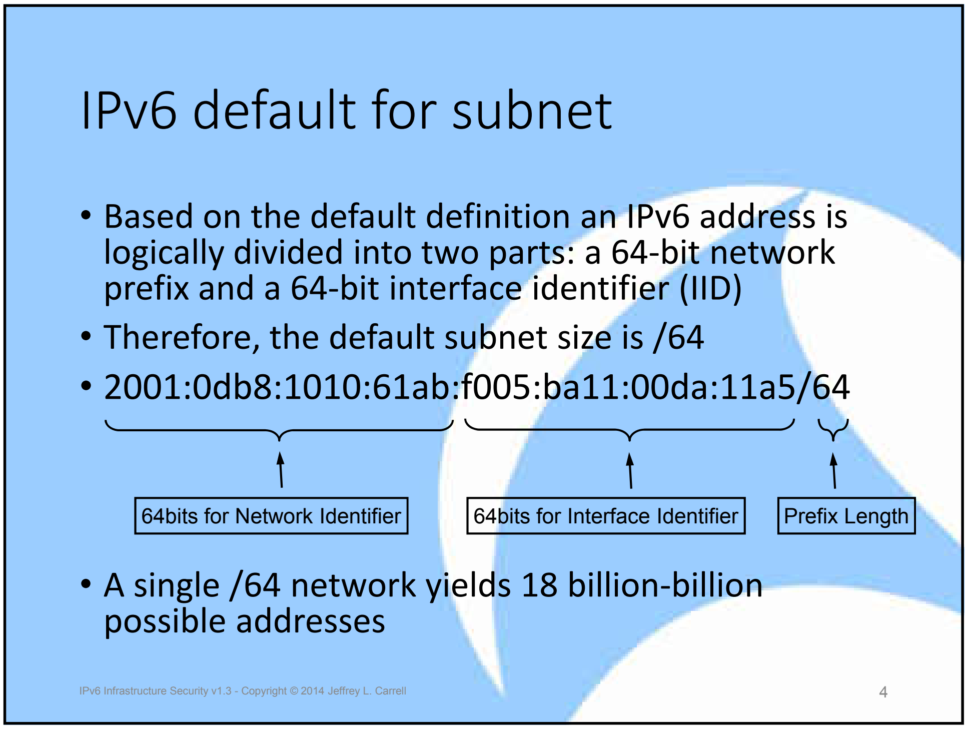
IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 2



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



IPv6 default for subnet

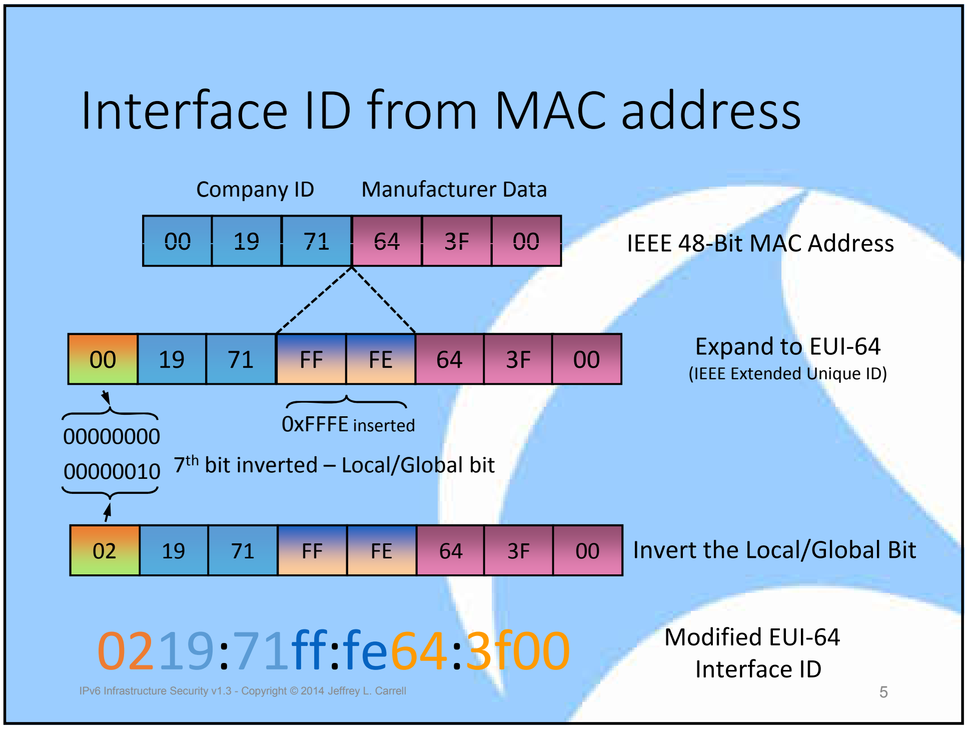
- Based on the default definition an IPv6 address is logically divided into two parts: a 64-bit network prefix and a 64-bit interface identifier (IID)
- Therefore, the default subnet size is /64
- 2001:0db8:1010:61ab:f005:ba11:00da:11a5/64

64bits for Network Identifier

64bits for Interface Identifier

Prefix Length

- A single /64 network yields 18 billion-billion possible addresses



Interface ID from MAC address

Company ID | Manufacturer Data

00	19	71	64	3F	00

IEEE 48-Bit MAC Address

00	19	71	FF	FE	64	3F	00

Expand to EUI-64
(IEEE Extended Unique ID)

0xFFFE inserted

00000000

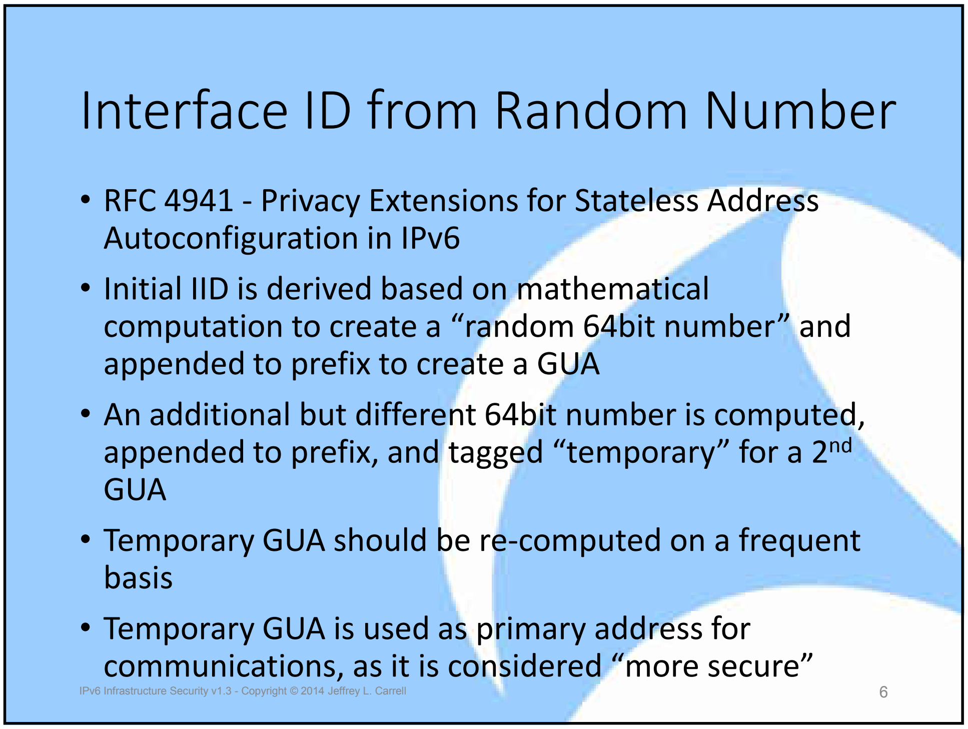
00000010 7th bit inverted – Local/Global bit

02	19	71	FF	FE	64	3F	00

Invert the Local/Global Bit

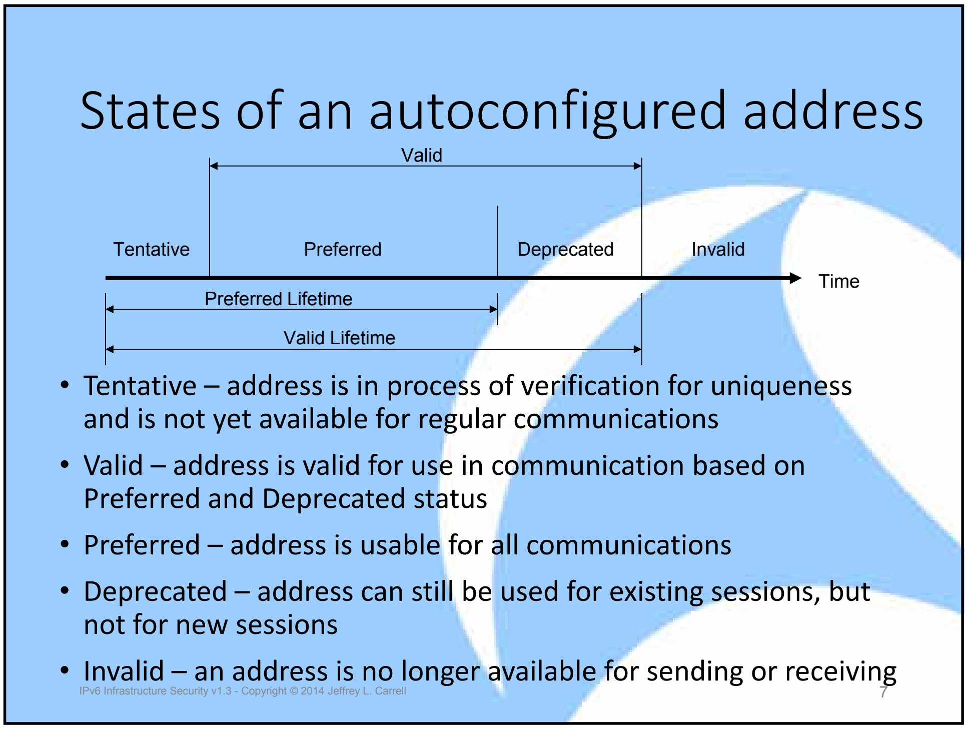
0219:71ff:fe64:3f00

Modified EUI-64
Interface ID



Interface ID from Random Number

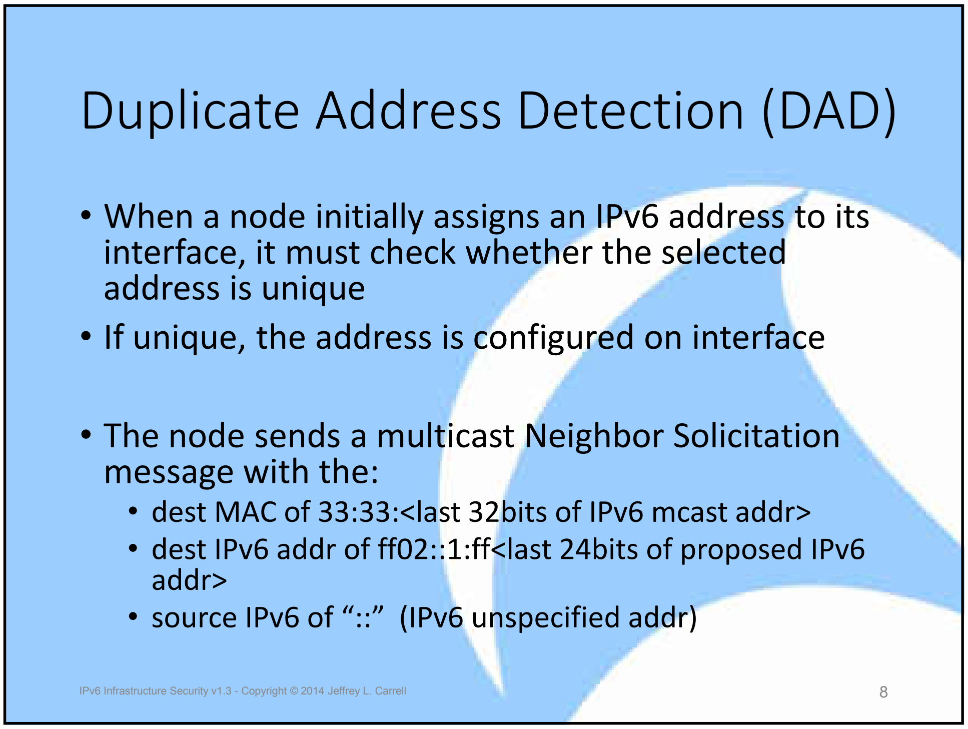
- RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- Initial IID is derived based on mathematical computation to create a “random 64bit number” and appended to prefix to create a GUA
- An additional but different 64bit number is computed, appended to prefix, and tagged “temporary” for a 2nd GUA
- Temporary GUA should be re-computed on a frequent basis
- Temporary GUA is used as primary address for communications, as it is considered “more secure”



States of an autoconfigured address

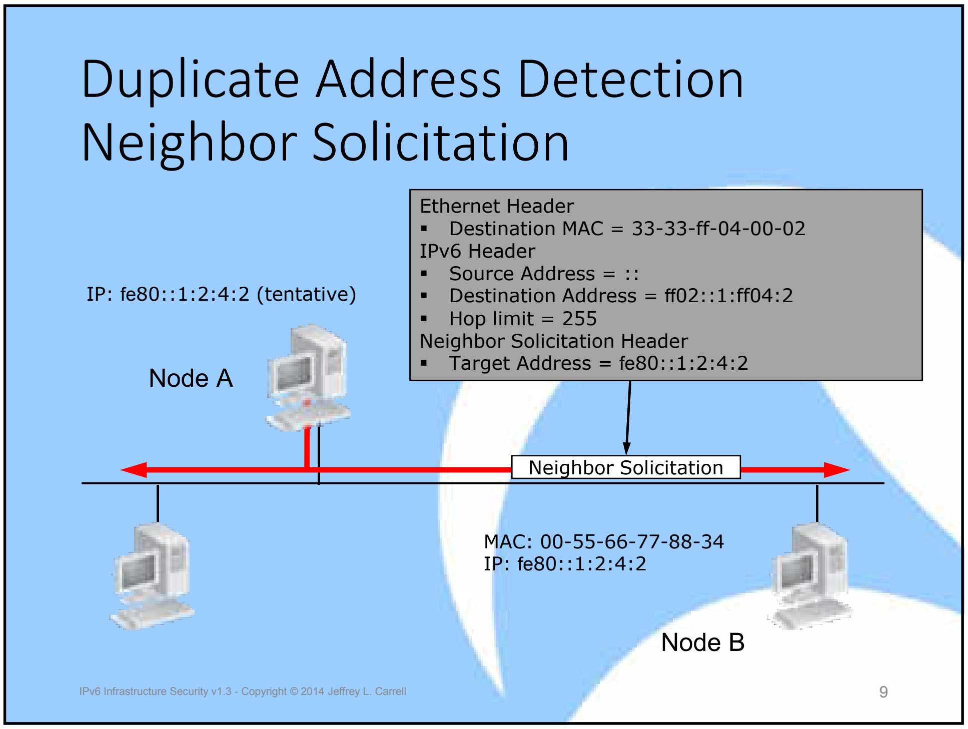
Valid
Tentative
Preferred
Deprecated
Invalid
Time
Preferred Lifetime
Valid Lifetime

- Tentative – address is in process of verification for uniqueness and is not yet available for regular communications
- Valid – address is valid for use in communication based on Preferred and Deprecated status
- Preferred – address is usable for all communications
- Deprecated – address can still be used for existing sessions, but not for new sessions
- Invalid – an address is no longer available for sending or receiving



Duplicate Address Detection (DAD)

- When a node initially assigns an IPv6 address to its interface, it must check whether the selected address is unique
- If unique, the address is configured on interface
- The node sends a multicast Neighbor Solicitation message with the:
  - dest MAC of 33:33:<last 32bits of IPv6 mcast addr>
  - dest IPv6 addr of ff02::1:ff<last 24bits of proposed IPv6 addr>
  - source IPv6 of "::" (IPv6 unspecified addr)



Duplicate Address Detection Neighbor Solicitation

Ethernet Header
- Destination MAC = 33-33-ff-04-00-02

IPv6 Header
- Source Address = ::
- Destination Address = ff02::1:ff04:2
- Hop limit = 255

Neighbor Solicitation Header
- Target Address = fe80::1:2:4:2

IP: fe80::1:2:4:2 (tentative)

Node A

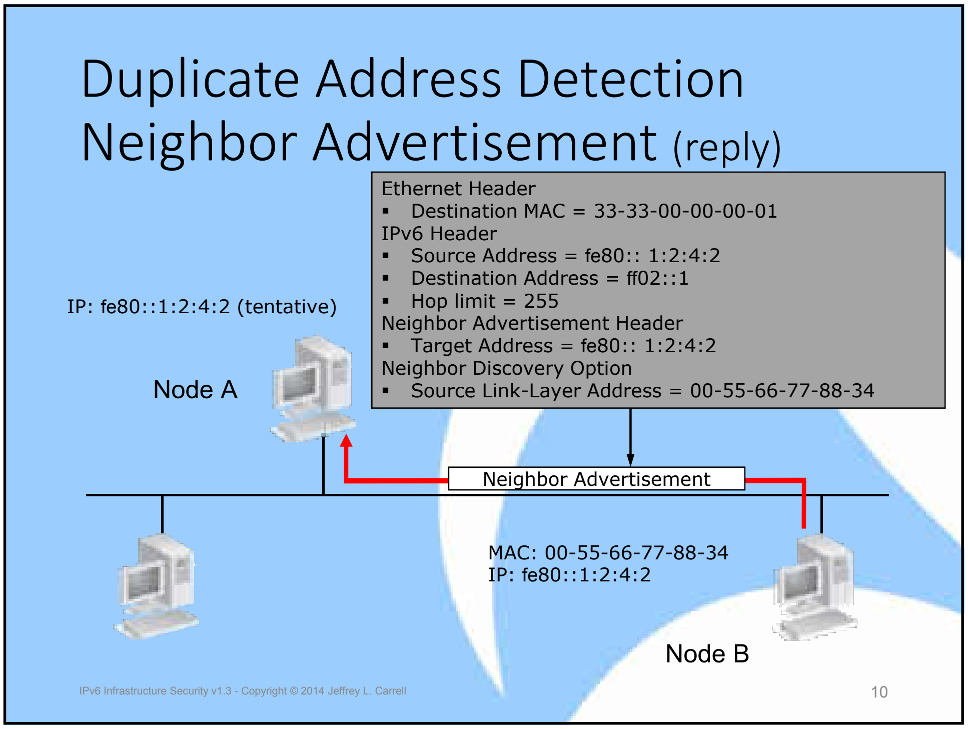
Neighbor Solicitation

MAC: 00-55-66-77-88-34
IP: fe80::1:2:4:2

Node B

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

9



Duplicate Address Detection Neighbor Advertisement (reply)

Ethernet Header
- Destination MAC = 33-33-00-00-00-01

IPv6 Header
- Source Address = fe80:: 1:2:4:2
- Destination Address = ff02::1
- Hop limit = 255

Neighbor Advertisement Header
- Target Address = fe80:: 1:2:4:2

Neighbor Discovery Option
- Source Link-Layer Address = 00-55-66-77-88-34

IP: fe80::1:2:4:2 (tentative)

Node A

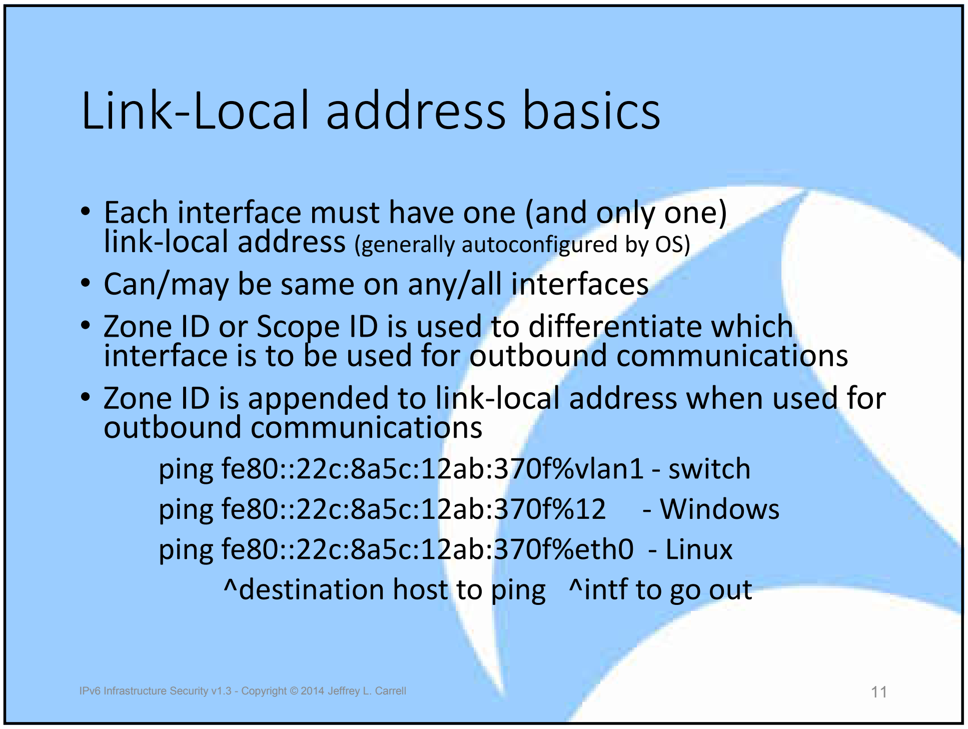
Neighbor Advertisement

MAC: 00-55-66-77-88-34
IP: fe80::1:2:4:2

Node B

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

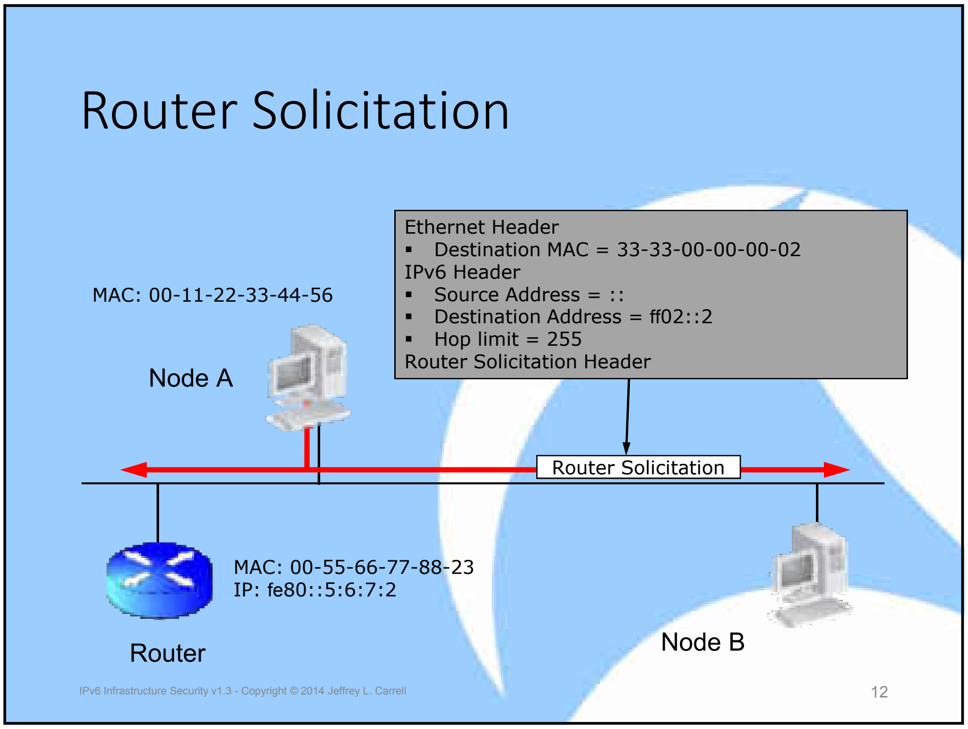
10



Link-Local address basics

- Each interface must have one (and only one) link-local address (generally autoconfigured by OS)
- Can/may be same on any/all interfaces
- Zone ID or Scope ID is used to differentiate which interface is to be used for outbound communications
- Zone ID is appended to link-local address when used for outbound communications

```
ping fe80::22c:8a5c:12ab:370f%vlan1 - switch
ping fe80::22c:8a5c:12ab:370f%12     - Windows
ping fe80::22c:8a5c:12ab:370f%eth0  - Linux
     ^destination host to ping   ^intf to go out
```

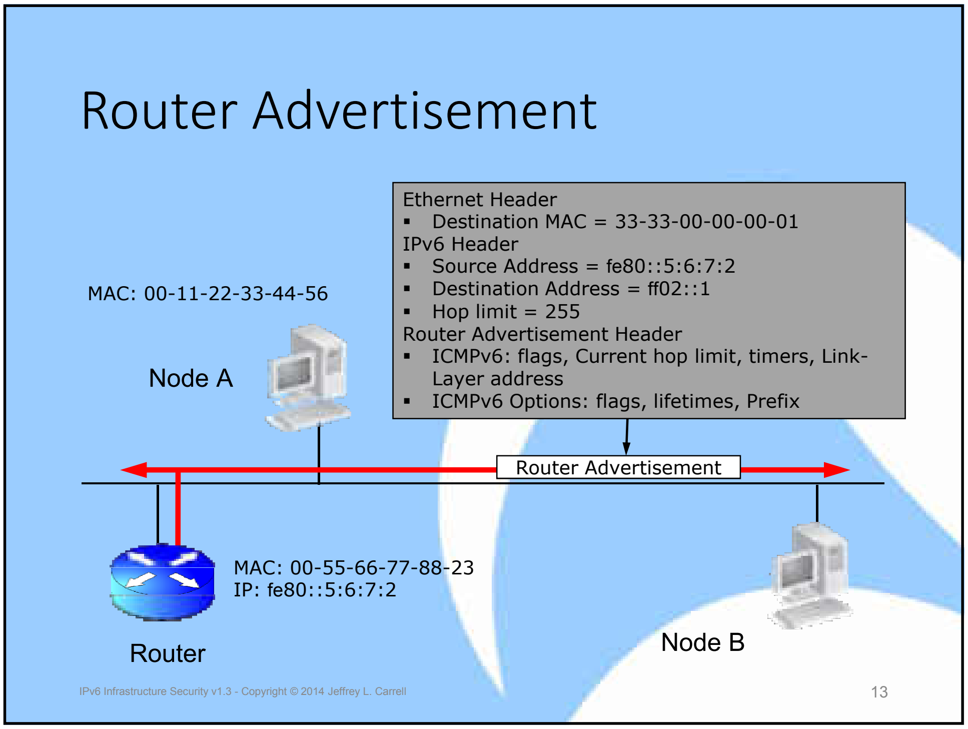


Router Solicitation

Ethernet Header
- Destination MAC = 33-33-00-00-00-02

IPv6 Header
- Source Address = ::
- Destination Address = ff02::2
- Hop limit = 255

Router Solicitation Header



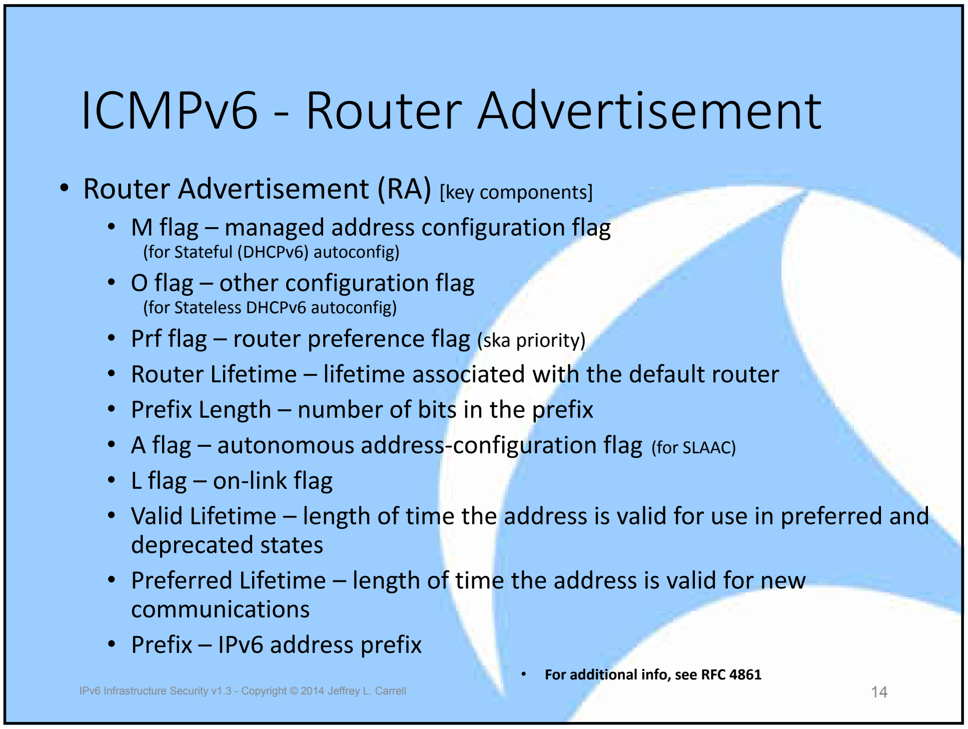
Router Advertisement

Ethernet Header
- Destination MAC = 33-33-00-00-00-01

IPv6 Header
- Source Address = fe80::5:6:7:2
- Destination Address = ff02::1
- Hop limit = 255

Router Advertisement Header
- ICMPv6: flags, Current hop limit, timers, Link-Layer address
- ICMPv6 Options: flags, lifetimes, Prefix

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 13



ICMPv6 - Router Advertisement

- Router Advertisement (RA) [key components]
  - M flag – managed address configuration flag
    (for Stateful (DHCPv6) autoconfig)
  - O flag – other configuration flag
    (for Stateless DHCPv6 autoconfig)
  - Prf flag – router preference flag (ska priority)
  - Router Lifetime – lifetime associated with the default router
  - Prefix Length – number of bits in the prefix
  - A flag – autonomous address-configuration flag (for SLAAC)
  - 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

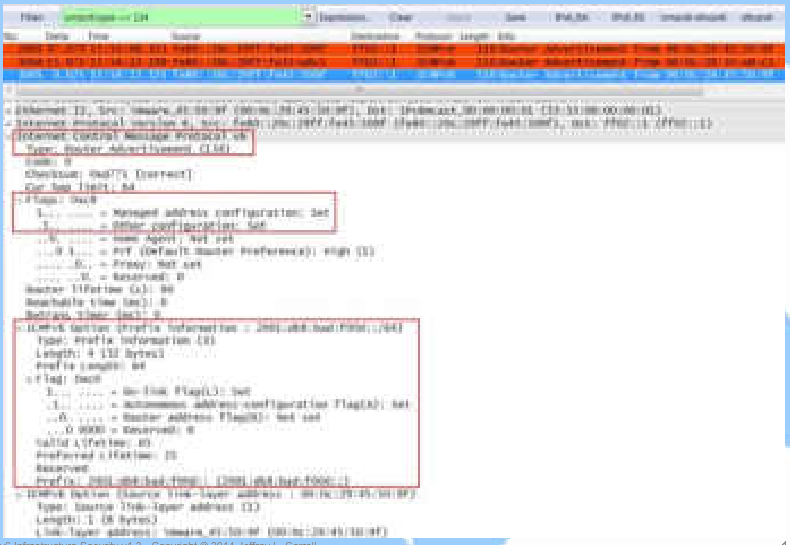
- **For additional info, see RFC 4861**

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 14

IPv6 autoconfiguration options

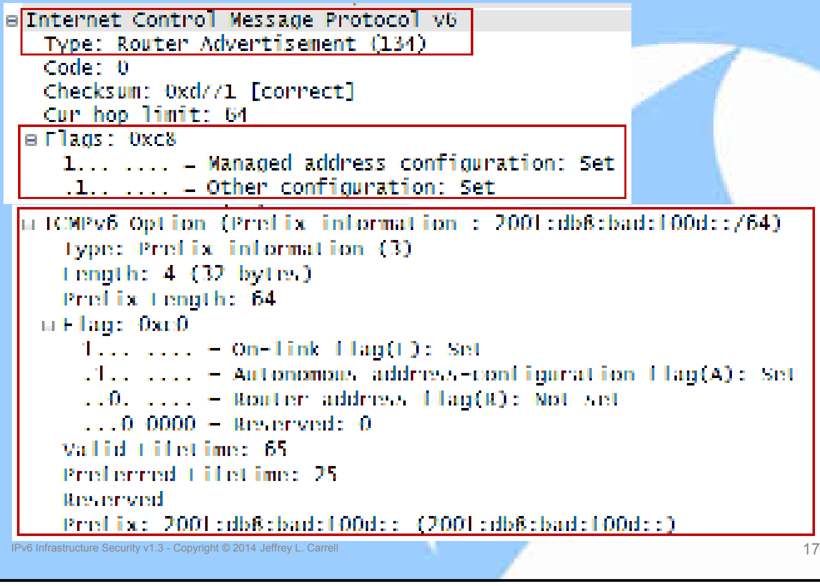
Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info		Prefix Derived from	Interface ID Derived from	Other Configuration Options (DNS, time, tftp, etc)	Number of IPv6 Addresses on interface
	M Flag	O Flag	A Flag	L Flag				
Link-Local (always configured)	N/A	N/A	N/A	N/A	Internal (fe80::/64)	M-EUI-64 or Privacy	Manual	1
Manual assigned	Off	Off	Off	On	Manual	Manual	Manual	2 (LL, manual)
SLAAC	Off	Off	On	On	RA	M-EUI-64 or Privacy	Manual	3 (LL, IPv6, IPv6 temp)
Stateful (DHCPv6)	On	N/R	Off	On	DHCPv6	DHCPv6	DHCPv6	2 (LL, DHCPv6)
Stateless DHCPv6	Off	On	On	On	RA	M-EUI-64 or Privacy	DHCPv6	3 (LL, IPv6, IPv6 temp)
Combination Stateless & DHCPv6	On	N/R	On	On	RA and DHCPv6	M-EUI-64 or Privacy and DHCPv6	DHCPv6	4 (LL, IPv6, IPv6 temp, DHCPv6)

Router Advertisement packet



```
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: [illegible] [correct]
  Cur hop limit: 64
- Flags: [illegible]
    1... .... = Managed address configuration: 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): [illegible]
  Reachable time (ms): 0
  Retrans timer (ms): 0
- ICMPv6 Option (Prefix information : 2001:db8:bad:f00d::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
  - Flag: [illegible]
      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: [illegible]
    Preferred Lifetime: [illegible]
    Reserved
    Prefix: 2001:db8:bad:f00d:: (2001:db8:bad:f00d::)
- ICMPv6 Option (Source link-layer address : [illegible])
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: [illegible]
```

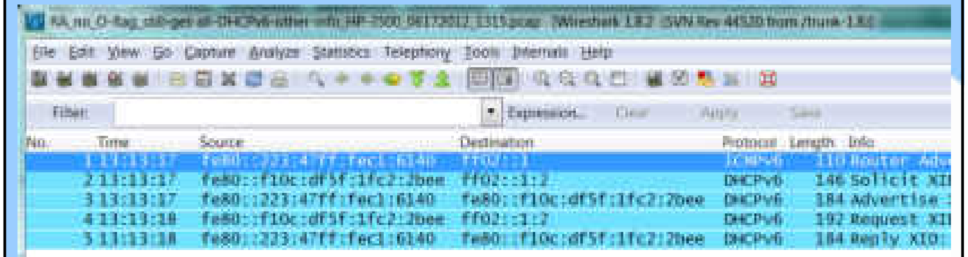
Router Advertisement packet



```
⊟ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xd771 [correct]
    Cur hop limit: 64
  ⊟ Flags: 0xc8
      1... .... = Managed address configuration: Set
      .1.. .... = Other configuration: Set
⊟ ICMPv6 Option (Prefix information : 2001:db8:bad:100d::/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: 65
      Preferred Lifetime: 25
      Reserved
      Prefix: 2001:db8:bad:100d:: (2001:db8:bad:100d::)
```

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 17

IPv6 Stateful (DHCPv6) process

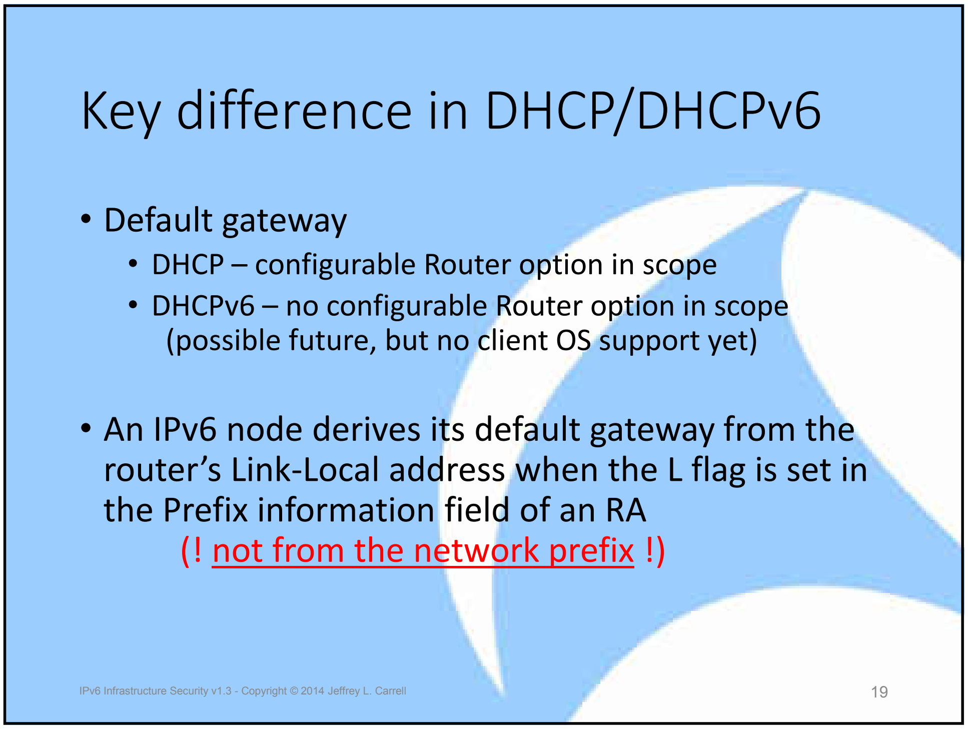


RA_m_O-flag_dhcp-get-all-DHCPv6-other-info_HP-2500_06172012_1315.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.   Time      Source                     Destination                Protocol Length Info
    1 13:13:17  fe80::223:47ff:fec1:6140   ff02::1                    ICMPv6    110 Router Adv
    2 13:13:17  fe80::f10c:df5f:1fc2:2bee  ff02::1:2                  DHCPv6    146 Solicit XID
    3 13:13:17  fe80::223:47ff:fec1:6140   fe80::f10c:df5f:1fc2:2bee  DHCPv6    184 Advertise
    4 13:13:18  fe80::f10c:df5f:1fc2:2bee  ff02::1:2                  DHCPv6    192 Request XID
    5 13:13:18  fe80::223:47ff:fec1:6140   fe80::f10c:df5f:1fc2:2bee  DHCPv6    184 Reply XID:
```

- DHCPv6**S**olicit = DHCP**D**iscover (IPv4)
- DHCPv6**A**dvertise = DHCP**O**ffer (IPv4)
- DHCPv6**R**equest = DHCP**R**equest (IPv4)
- DHCPv6**R**eply = DHCP**A**ck (IPv4)

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 18



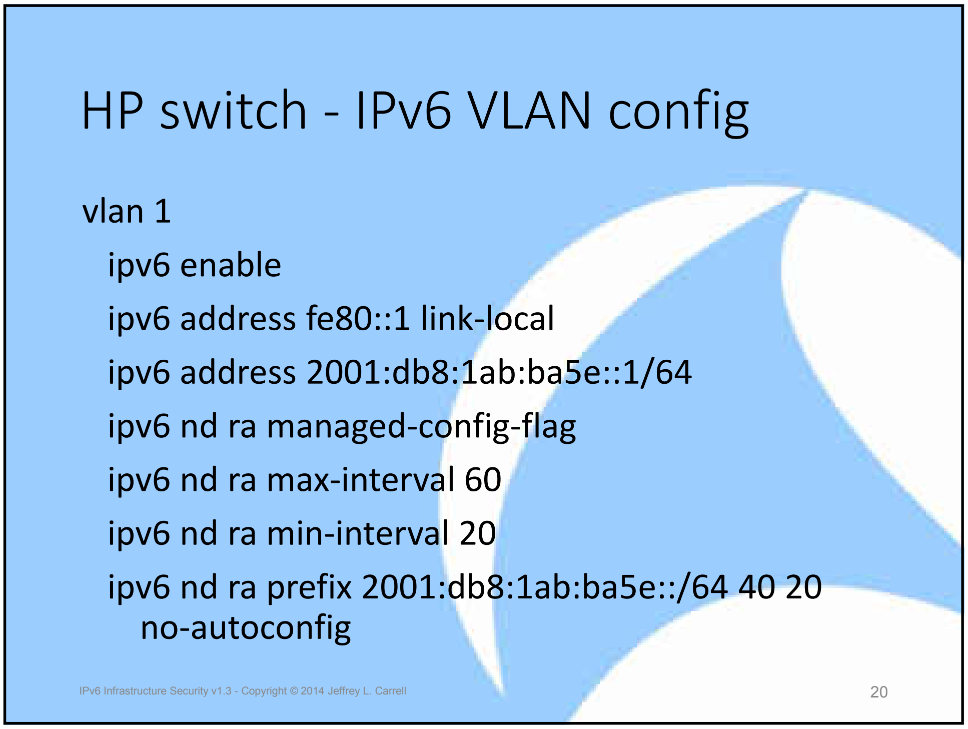
Key difference in DHCP/DHCPv6

- Default gateway
  - DHCP – configurable Router option in scope
  - DHCPv6 – no configurable Router option in scope (possible future, but no client OS support yet)
- 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 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

19

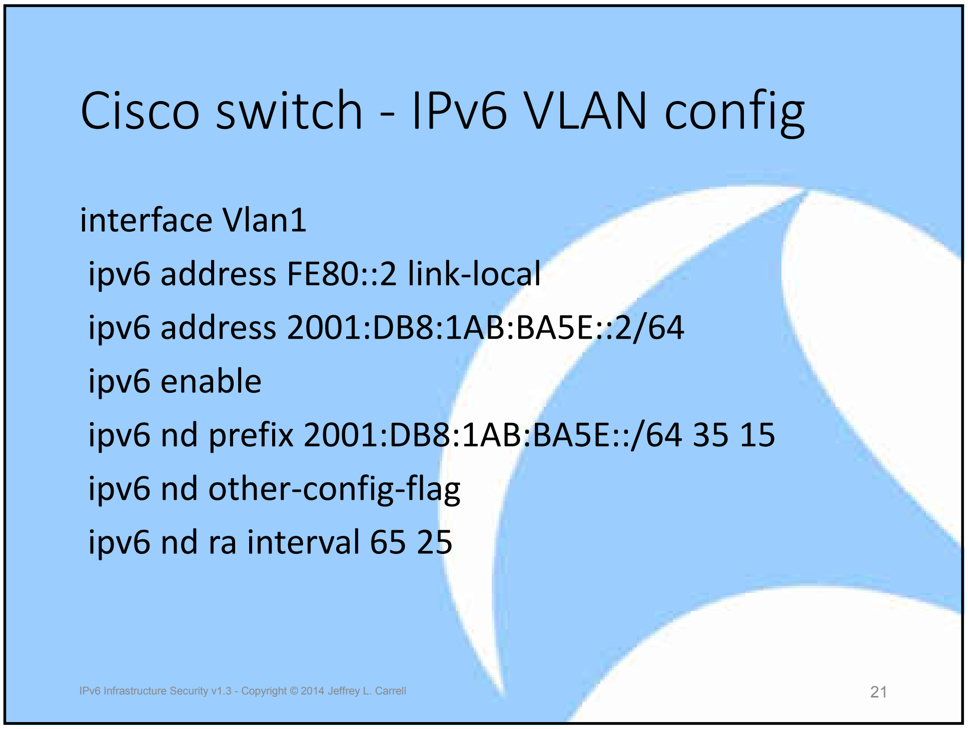


HP switch - IPv6 VLAN config

```
vlan 1
  ipv6 enable
  ipv6 address fe80::1 link-local
  ipv6 address 2001:db8:1ab:ba5e::1/64
  ipv6 nd ra managed-config-flag
  ipv6 nd ra max-interval 60
  ipv6 nd ra min-interval 20
  ipv6 nd ra prefix 2001:db8:1ab:ba5e::/64 40 20
     no-autoconfig
```

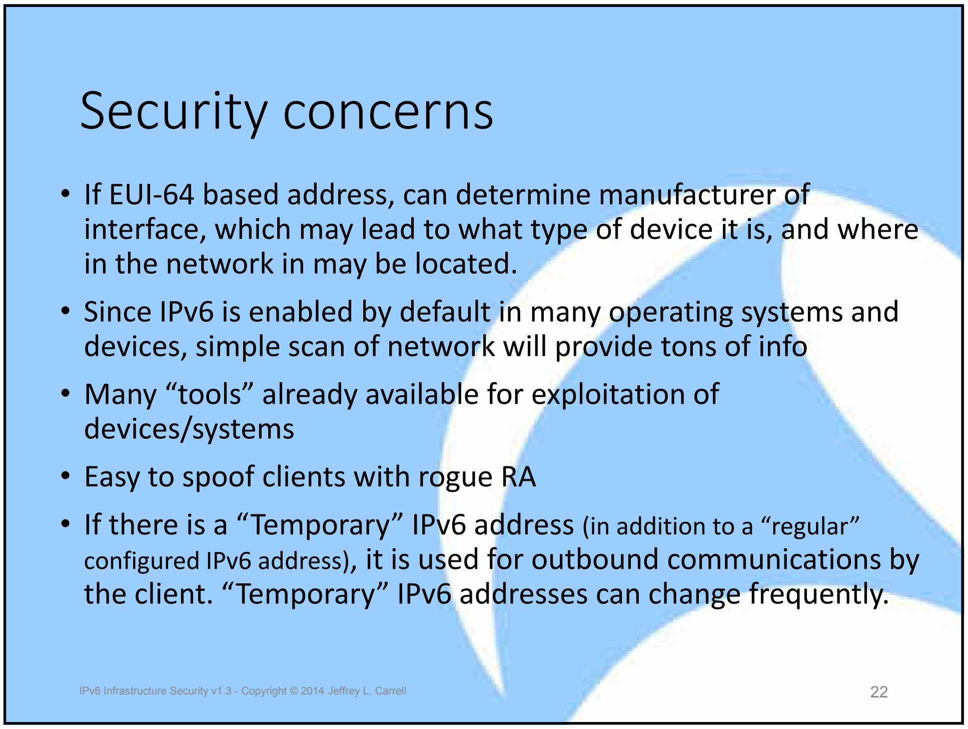
IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

20



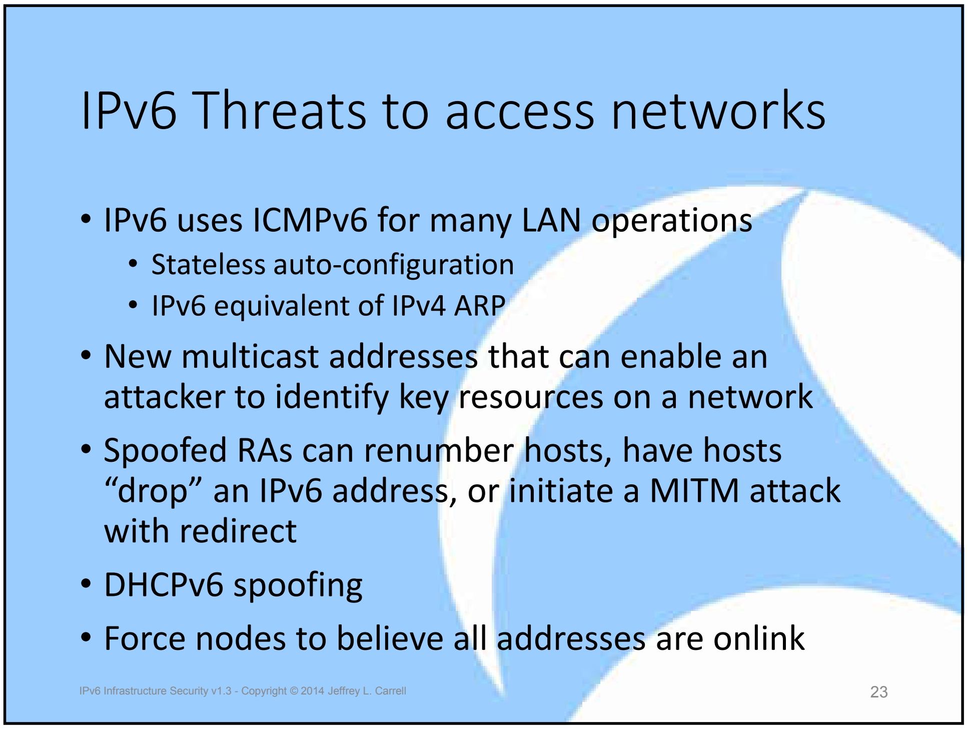
Cisco switch - IPv6 VLAN config

```
interface Vlan1
 ipv6 address FE80::2 link-local
 ipv6 address 2001:DB8:1AB:BA5E::2/64
 ipv6 enable
 ipv6 nd prefix 2001:DB8:1AB:BA5E::/64 35 15
 ipv6 nd other-config-flag
 ipv6 nd ra interval 65 25
```



Security concerns

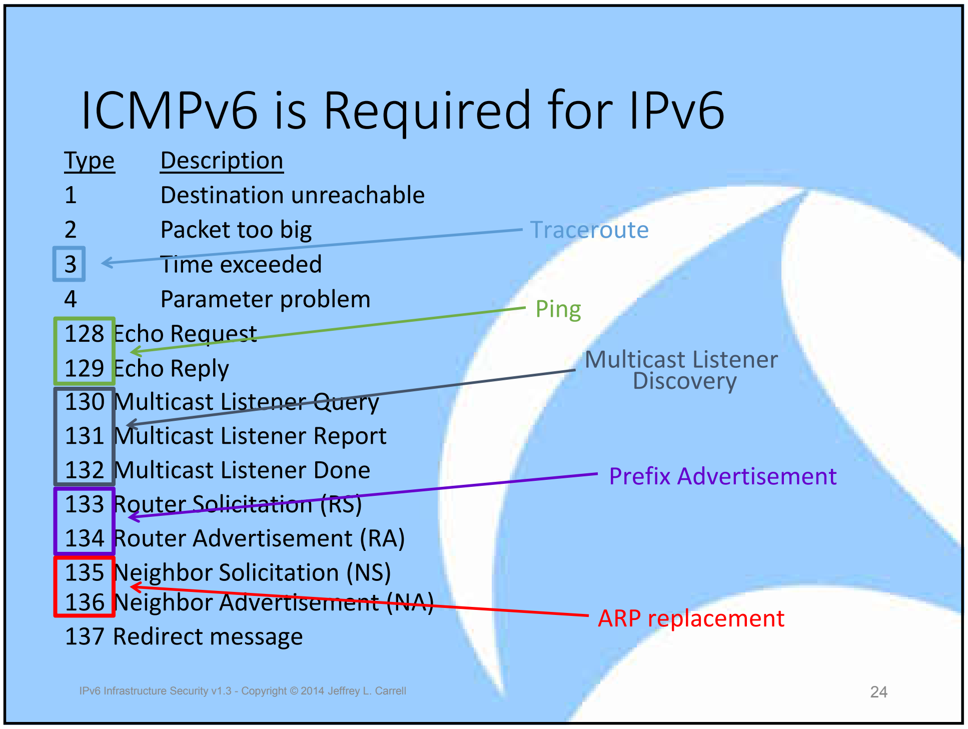
- If EUI-64 based address, can determine manufacturer of interface, which may lead to what type of device it is, and where in the network in may be located.
- Since IPv6 is enabled by default in many operating systems and devices, simple scan of network will provide tons of info
- Many “tools” already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



IPv6 Threats to access networks

- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - IPv6 equivalent of IPv4 ARP
- New multicast addresses that can enable an attacker to identify key resources on a network
- Spoofed RAs can renumber hosts, have hosts “drop” an IPv6 address, or initiate a MITM attack with redirect
- DHCPv6 spoofing
- Force nodes to believe all addresses are onlink

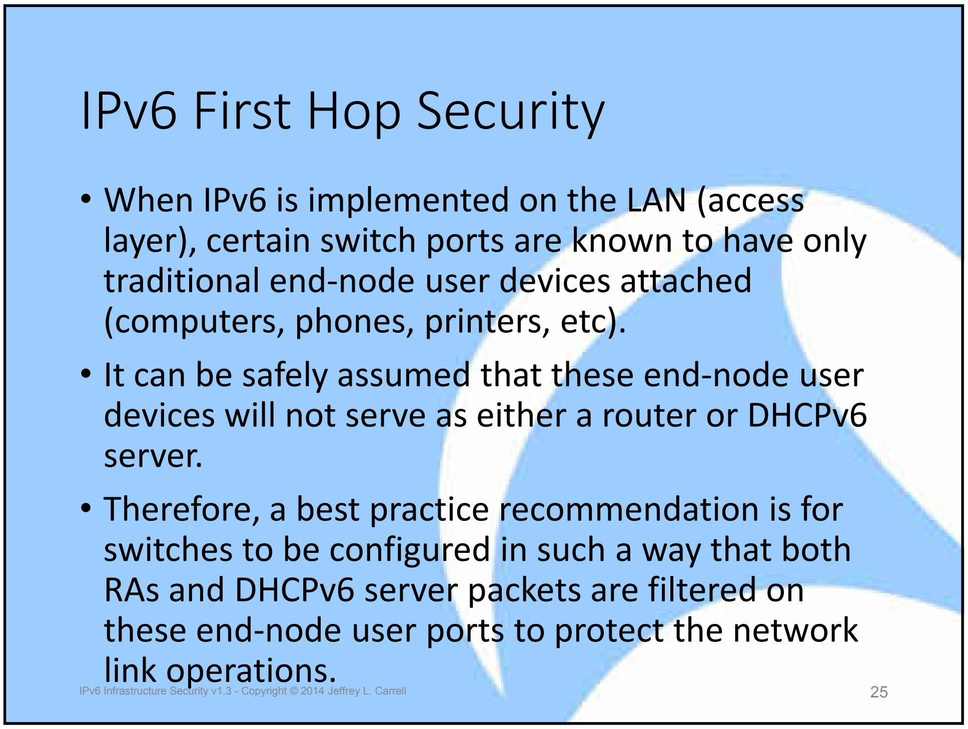
IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 23



ICMPv6 is Required for IPv6

Type	Description
1	Destination unreachable
2	Packet too big
3	Time exceeded
4	Parameter problem
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation (RS)
134	Router Advertisement (RA)
135	Neighbor Solicitation (NS)
136	Neighbor Advertisement (NA)
137	Redirect message

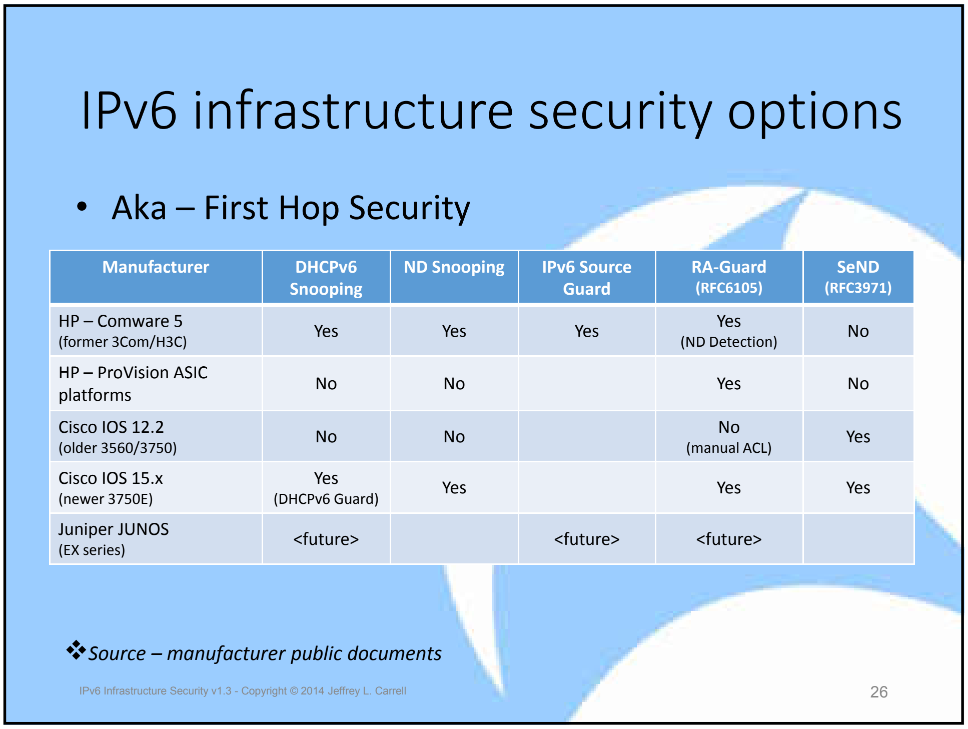
IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 24



IPv6 First Hop Security

- When IPv6 is implemented on the LAN (access layer), certain switch ports are known to have only traditional end-node user devices attached (computers, phones, printers, etc).
- It can be safely assumed that these end-node user devices will not serve as either a router or DHCPv6 server.
- Therefore, a best practice recommendation is for switches to be configured in such a way that both RAs and DHCPv6 server packets are filtered on these end-node user ports to protect the network link operations.

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 25



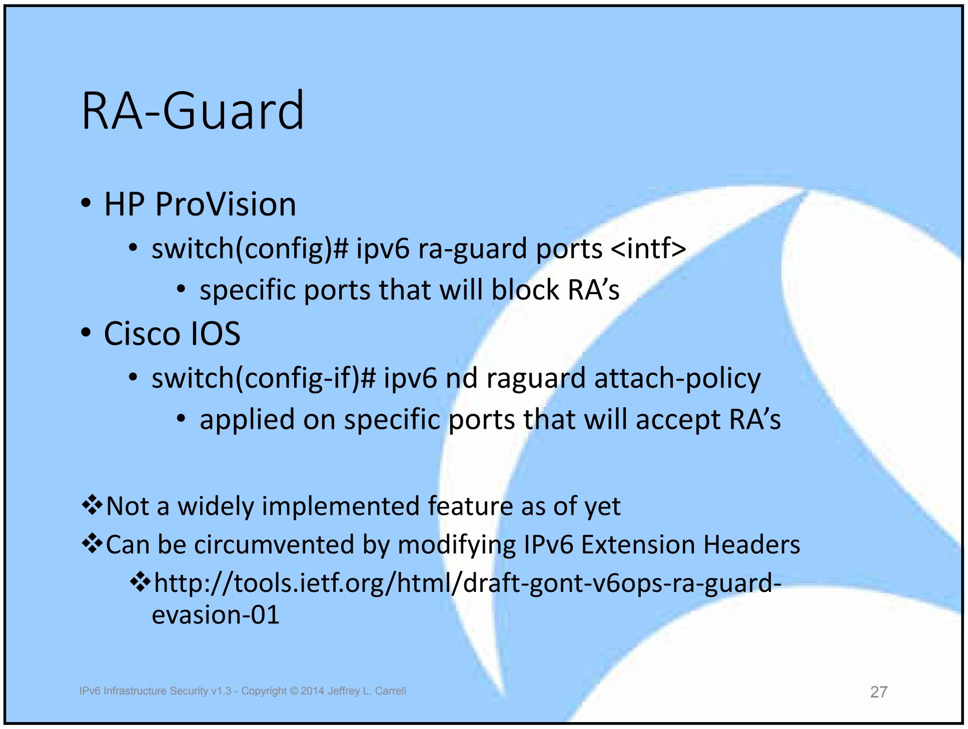
IPv6 infrastructure security options

- Aka – First Hop Security

Manufacturer	DHCPv6 Snooping	ND Snooping	IPv6 Source Guard	RA-Guard (RFC6105)	SeND (RFC3971)
HP – Comware 5 (former 3Com/H3C)	Yes	Yes	Yes	Yes (ND Detection)	No
HP – ProVision ASIC platforms	No	No		Yes	No
Cisco IOS 12.2 (older 3560/3750)	No	No		No (manual ACL)	Yes
Cisco IOS 15.x (newer 3750E)	Yes (DHCPv6 Guard)	Yes		Yes	Yes
Juniper JUNOS (EX series)	<future>		<future>	<future>	

❖*Source – manufacturer public documents*

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 26



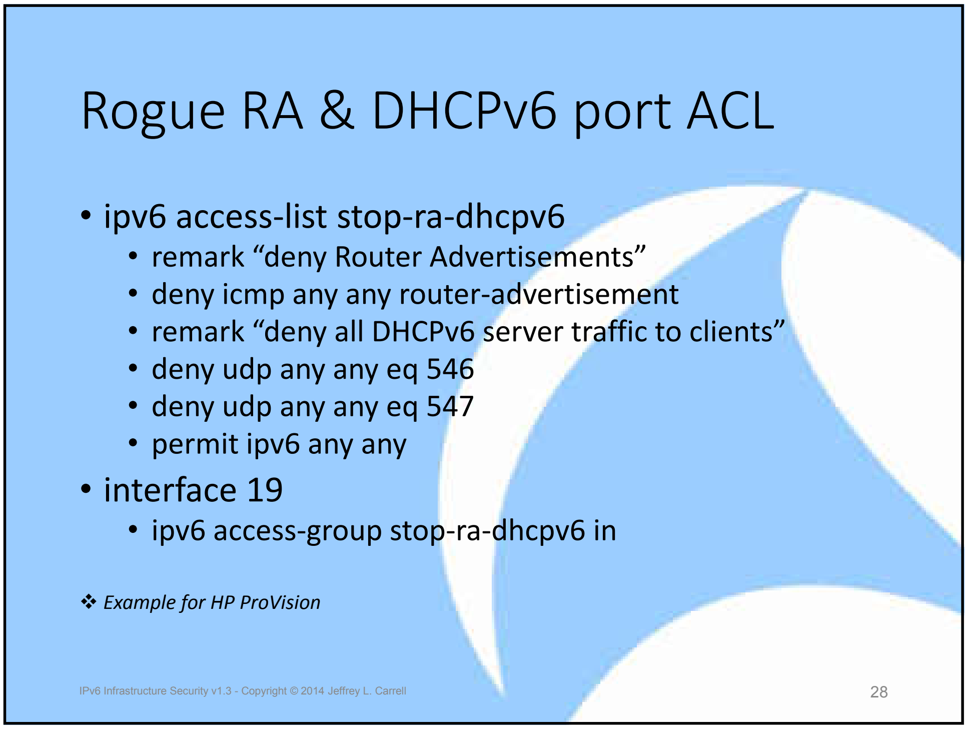
RA-Guard

- HP ProVision
  - switch(config)# ipv6 ra-guard ports <intf>
    - specific ports that will block RA's
- Cisco IOS
  - switch(config-if)# ipv6 nd raguard attach-policy
    - applied on specific ports that will accept RA's

❖Not a widely implemented feature as of yet

❖Can be circumvented by modifying IPv6 Extension Headers

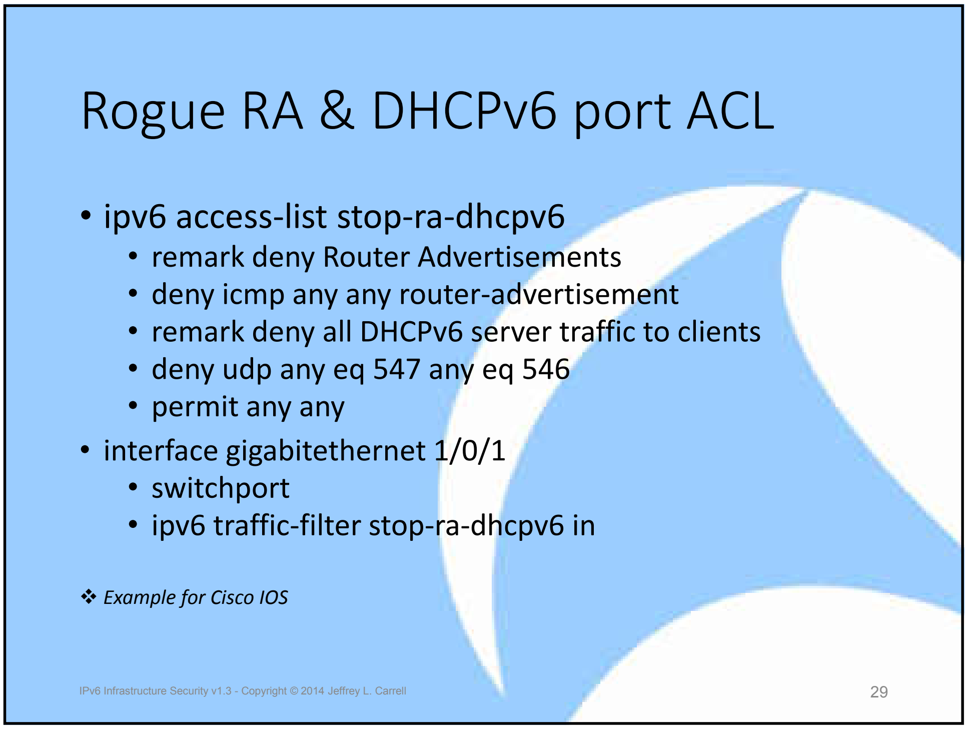
❖http://tools.ietf.org/html/draft-gont-v6ops-ra-guard-evasion-01



Rogue RA & DHCPv6 port ACL

- ipv6 access-list stop-ra-dhcpv6
  - remark "deny Router Advertisements"
  - deny icmp any any router-advertisement
  - remark "deny all DHCPv6 server traffic to clients"
  - deny udp any any eq 546
  - deny udp any any eq 547
  - permit ipv6 any any
- interface 19
  - ipv6 access-group stop-ra-dhcpv6 in

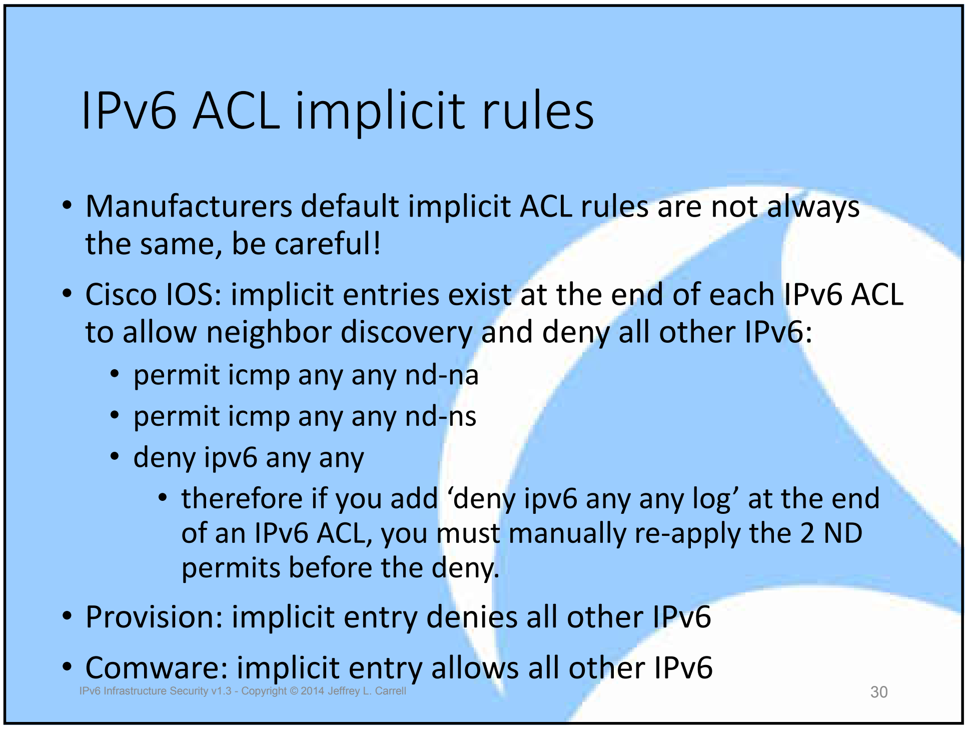
❖ *Example for HP ProVision*



Rogue RA & DHCPv6 port ACL

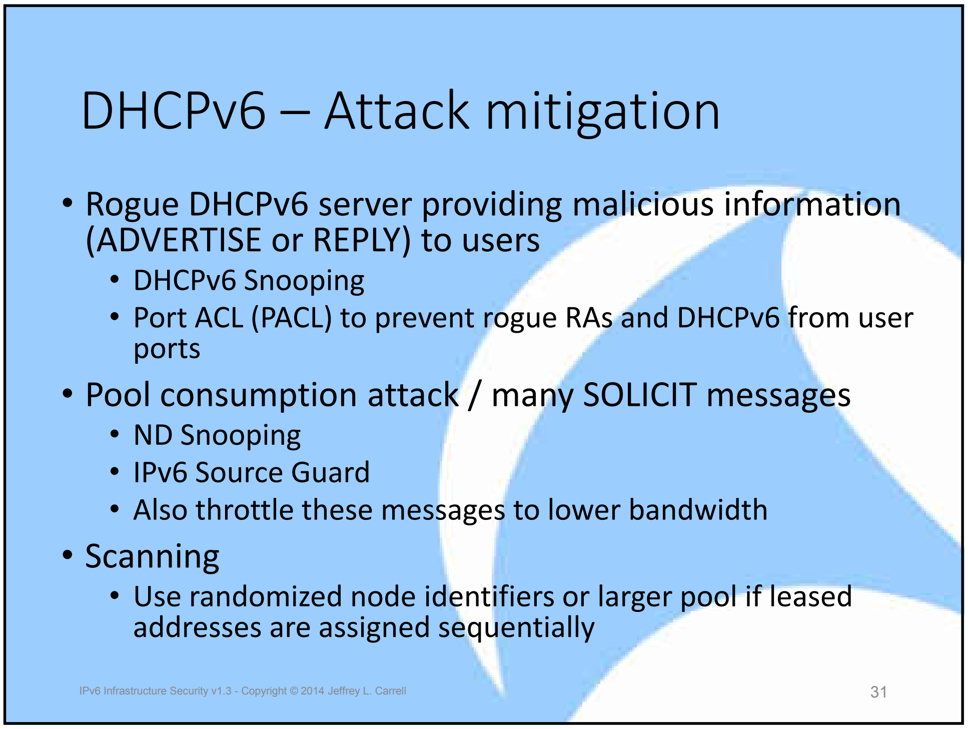
- ipv6 access-list stop-ra-dhcpv6
  - remark deny Router Advertisements
  - deny icmp any any router-advertisement
  - remark deny all DHCPv6 server traffic to clients
  - deny udp any eq 547 any eq 546
  - permit any any
- interface gigabitethernet 1/0/1
  - switchport
  - ipv6 traffic-filter stop-ra-dhcpv6 in

❖ *Example for Cisco IOS*



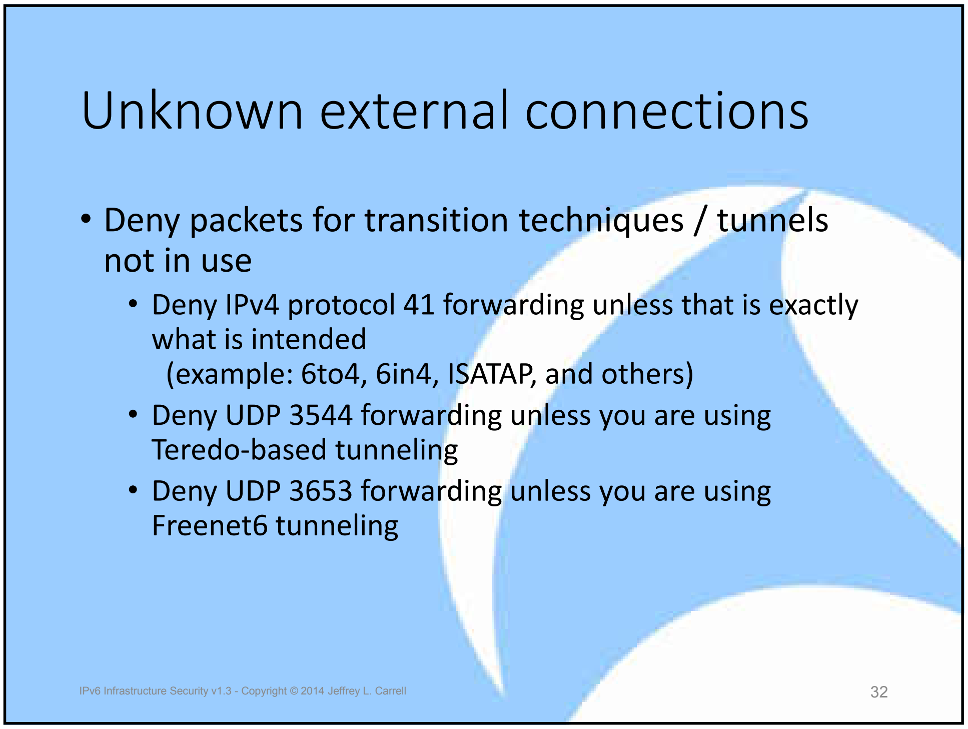
IPv6 ACL implicit rules

- Manufacturers default implicit ACL rules are not always the same, be careful!
- Cisco IOS: implicit entries exist at the end of each IPv6 ACL to allow neighbor discovery and deny all other IPv6:
  - permit icmp any any nd-na
  - permit icmp any any nd-ns
  - deny ipv6 any any
    - therefore if you add 'deny ipv6 any any log' at the end of an IPv6 ACL, you must manually re-apply the 2 ND permits before the deny.
- Provision: implicit entry denies all other IPv6
- Comware: implicit entry allows all other IPv6



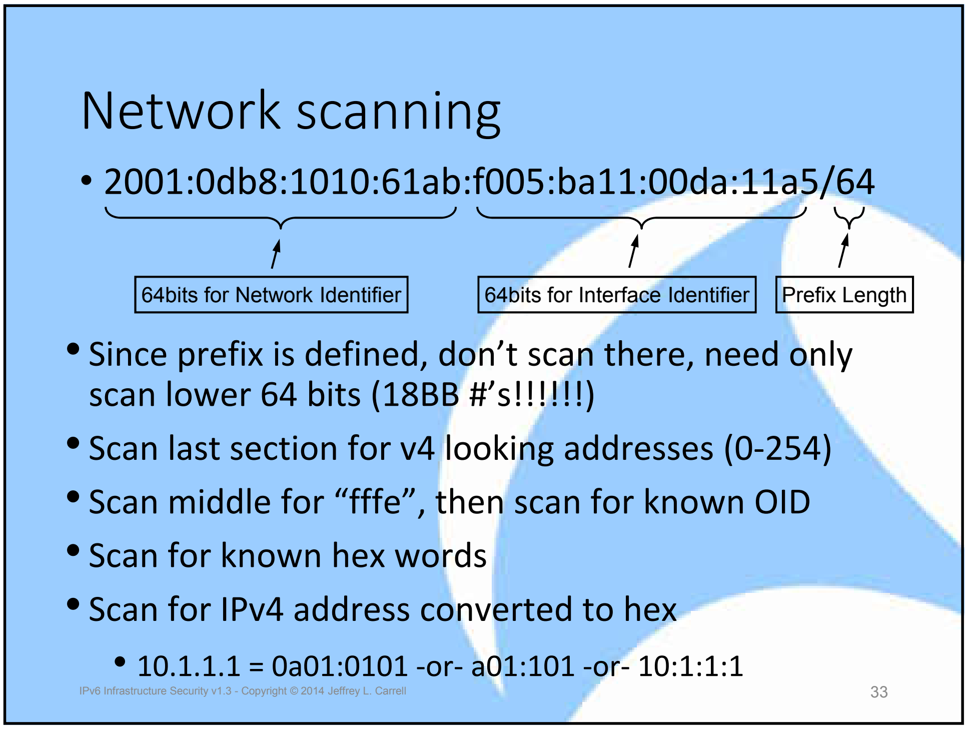
DHCPv6 – Attack mitigation

- Rogue DHCPv6 server providing malicious information (ADVERTISE or REPLY) to users
  - DHCPv6 Snooping
  - Port ACL (PACL) to prevent rogue RAs and DHCPv6 from user ports
- Pool consumption attack / many SOLICIT messages
  - ND Snooping
  - IPv6 Source Guard
  - Also throttle these messages to lower bandwidth
- Scanning
  - Use randomized node identifiers or larger pool if leased addresses are assigned sequentially



Unknown external connections

- Deny packets for transition techniques / tunnels not in use
  - Deny IPv4 protocol 41 forwarding unless that is exactly what is intended
    (example: 6to4, 6in4, ISATAP, and others)
  - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling
  - Deny UDP 3653 forwarding unless you are using Freenet6 tunneling



Network scanning

- 2001:0db8:1010:61ab:f005:ba11:00da:11a5/64

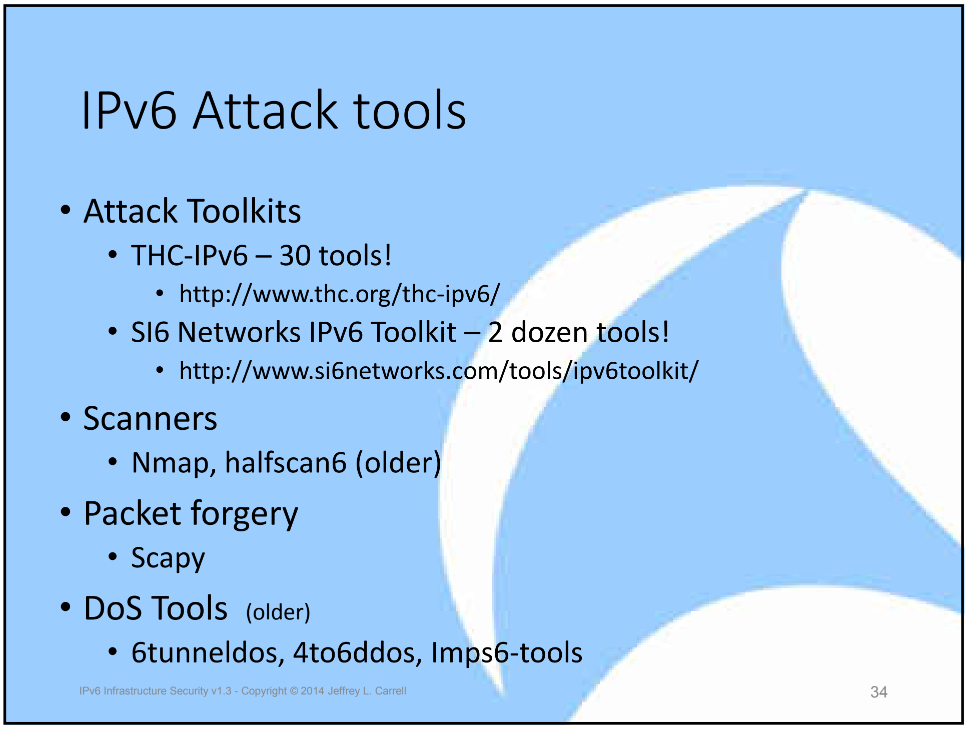
64bits for Network Identifier

64bits for Interface Identifier

Prefix Length

- Since prefix is defined, don’t scan there, need only scan lower 64 bits (18BB #’s!!!!!!)
- Scan last section for v4 looking addresses (0-254)
- Scan middle for “fffe”, then scan for known OID
- Scan for known hex words
- Scan for IPv4 address converted to hex
  - 10.1.1.1 = 0a01:0101 -or- a01:101 -or- 10:1:1:1

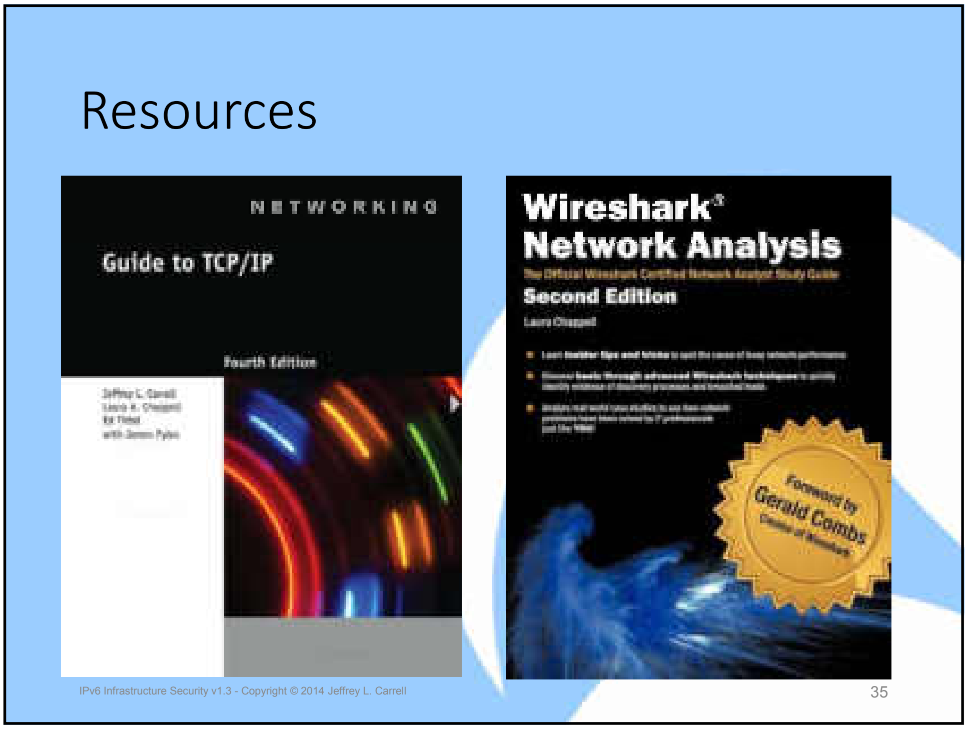
IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 33



IPv6 Attack tools

- Attack Toolkits
  - THC-IPv6 – 30 tools!
    - http://www.thc.org/thc-ipv6/
  - SI6 Networks IPv6 Toolkit – 2 dozen tools!
    - http://www.si6networks.com/tools/ipv6toolkit/
- Scanners
  - Nmap, halfscan6 (older)
- Packet forgery
  - Scapy
- DoS Tools (older)
  - 6tunneldos, 4to6ddos, Imps6-tools

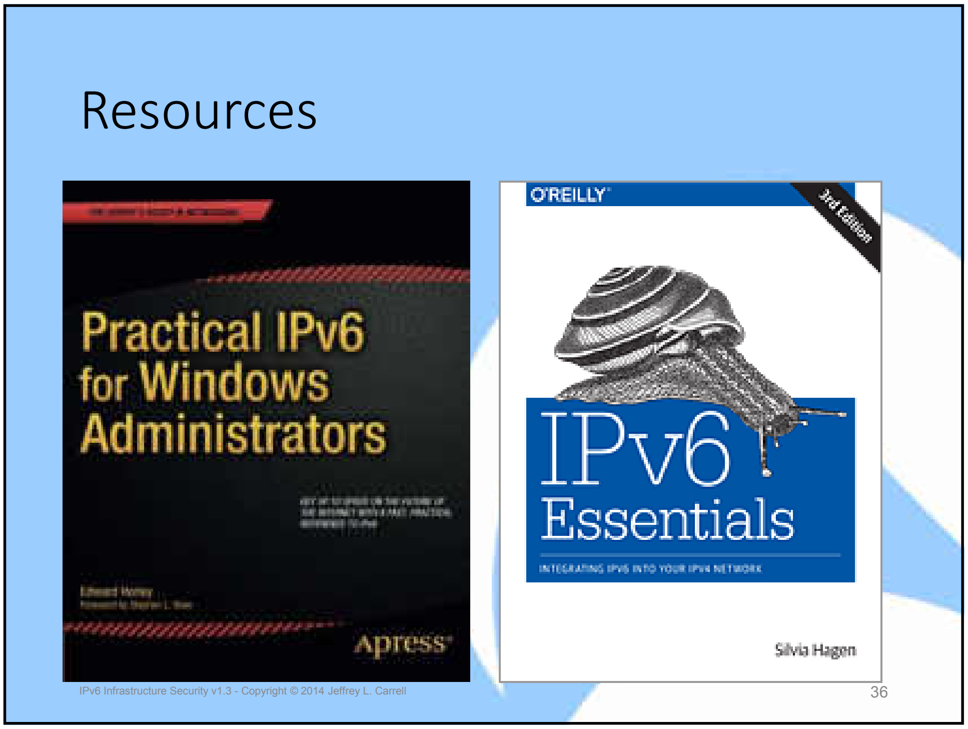
IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell 34



Resources

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

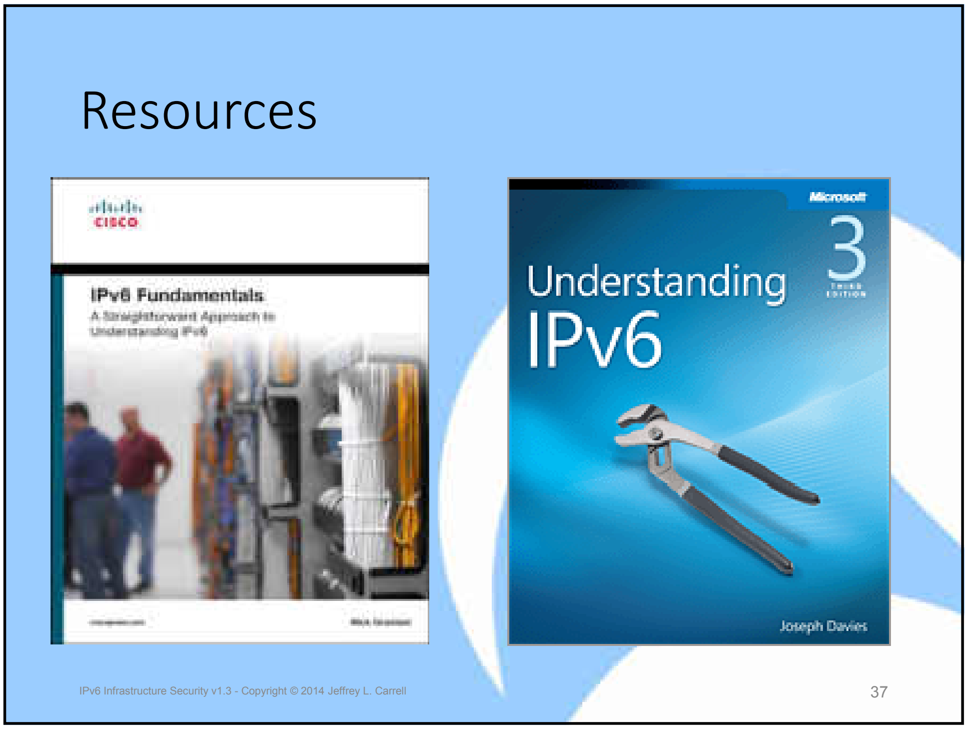
35



Resources

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

36



Resources

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

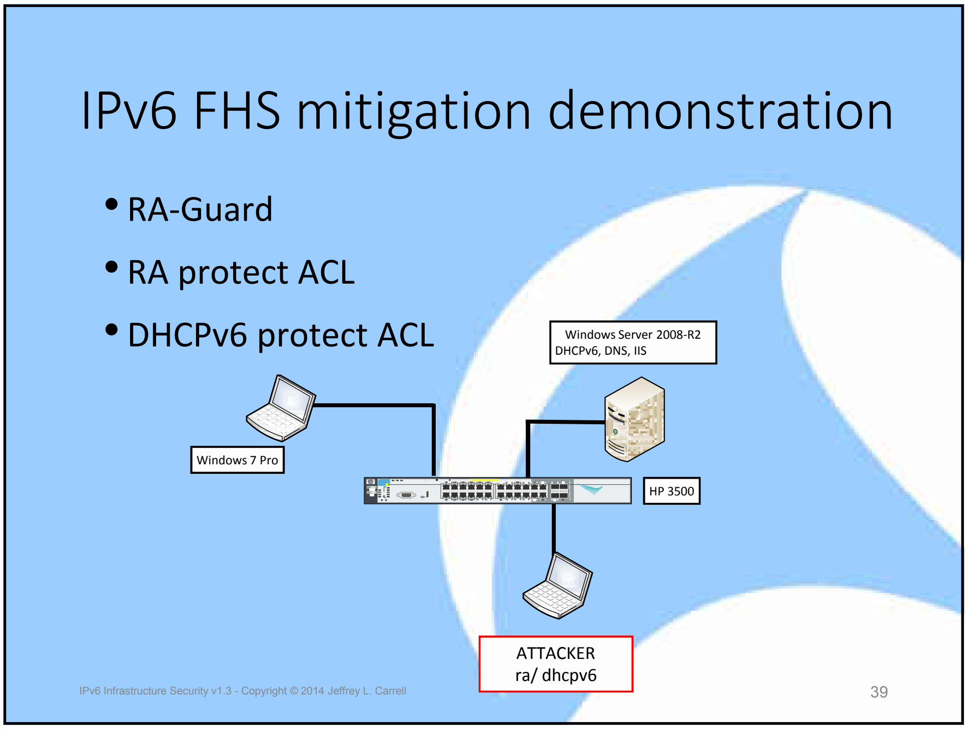
37

Resources

cisco
SECURITY
IPv6 Security
cisco
IPv6 for Enterprise Networks

IPv6 Infrastructure Security v1.3 - Copyright © 2014 Jeffrey L. Carrell

38



IPv6 FHS mitigation demonstration

- RA-Guard
- RA protect ACL
- DHCPv6 protect ACL

Windows Server 2008-R2
DHCPv6, DNS, IIS

Windows 7 Pro

HP 3500

ATTACKER
ra/ dhcpv6

SHARKFEST '14
WIRESHARK DEVELOPER AND USER CONFERENCE
JUNE 16-20 2014 · DOMINICAN UNIVERSITY

Thank You for Attending

Jeffrey L Carrell
Network Security Consultant , IPv6 SME/Trainer
jeff.carrell@teachmeipv6.com
jeff.carrell@networkconversions.com
@JeffCarrell_v6

IPv6 FORUM
CERTIFIED
ENGINEER
IPv6 FORUM
CERTIFIED
TRAINER

Certificate of Completion
jeffcarrell
hereby awarded the rank of
Sage
Hurricane Electric
IPv6 Certification

IPv6 Infrastructure Security v1.3