IPv6 Infrastructure Security

2013 North American IPv6 Summit

Jeffrey L Carrell

Network Conversions

Network Security Consultant
IPv6 SME/Trainer

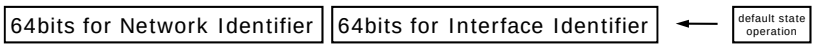
Agenda

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

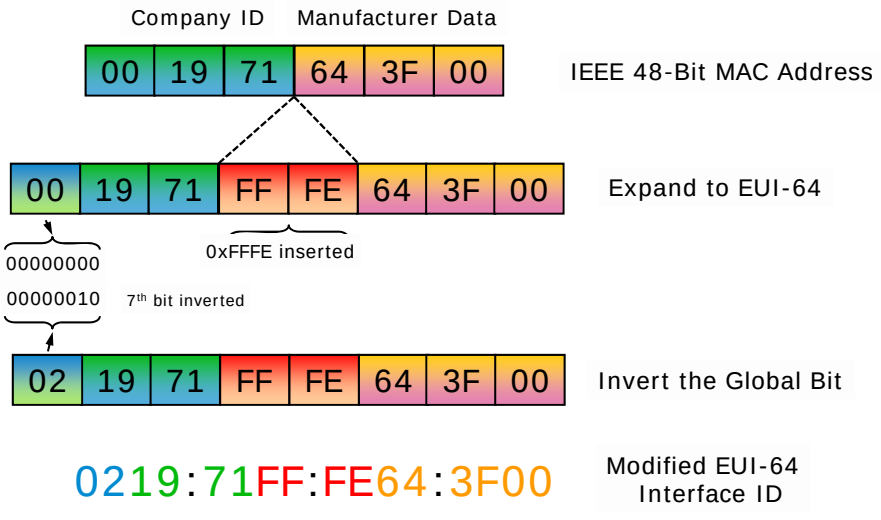
What is an IPv6 Address?

- 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!!!

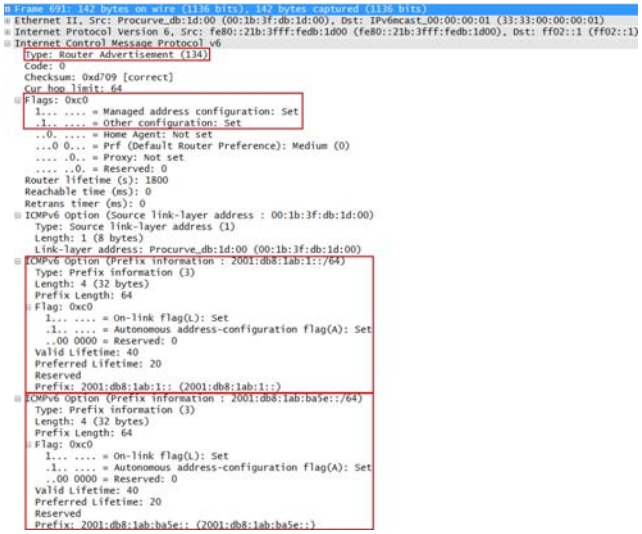
ICMPv6 - Router Advertisement

- Router Advertisement (RA) [key components]
  - M flag – managed address configuration flag
    (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 autoconfiguration options

Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags M Flag	O Flag	ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info A Flag	L Flag	Prefix Derived from	Interface ID Derived from	Other Configuration Options (DNS, time, tftp, etc)	Number of IPv6 Addresses on interface
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



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::/10, assigned as 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)

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 A & L flags "on" and 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
- Note – no DNS automatically configured

IPv6 Stateful (DHCPv6) process

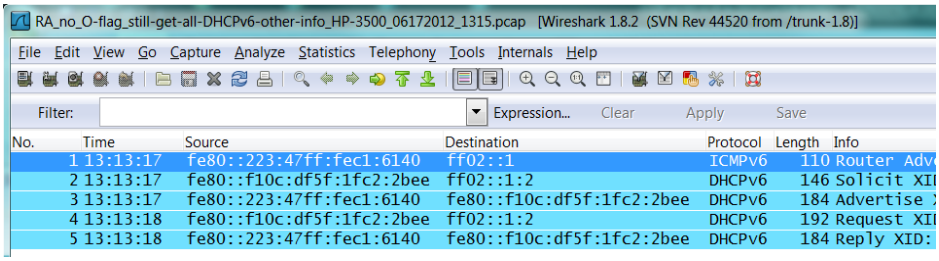
- A node sends a multicast Router Solicitation message to the "all-routers" address FF02::2
- Router(s) respond with Router Advertisement message containing M & L flags "on" for stateful autoconfiguration
- The node sends a multicast Solicit message to the "all-DHCP relay agents and servers" address 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

Router Advertisement packet (Stateful/DHCPv6)

```
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)
```

IPv6 Stateful (DHCPv6) process



- 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)

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 !)

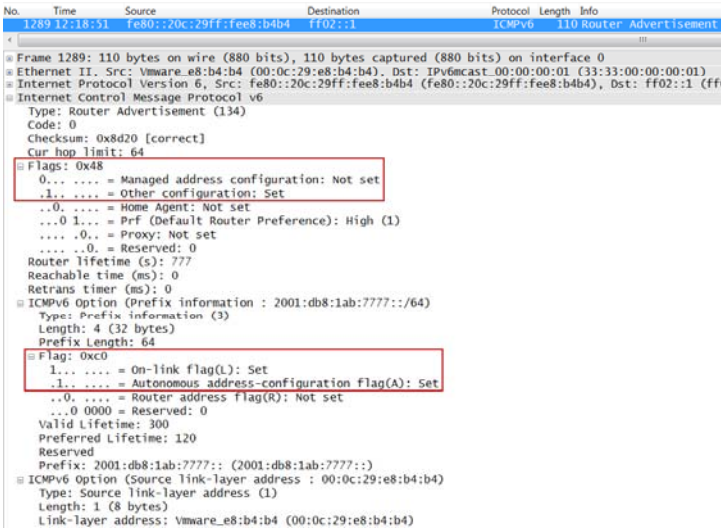
IPv6 address autoconfiguration, con't

- 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, time server, tftp or download server, etc

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 A & L flags "on" and prefix(es), and O flag "on" 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

Router Advertisement packet (Stateless DHCPv6)



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

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

Traceroute
Ping
Multicast Listener Discovery
Prefix Advertisement
ARP replacement

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 options, aka First Hop Security

- Some common access layer platforms

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*

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 widely implemented 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 all traffic DHCPv6 server to client
  - deny udp any eq 547 any eq 546
  - remark deny Router Advertisements
  - deny icmp any any router-advertisement
  - 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 only 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 – unless using 6to4 tunneling
  - Deny UDP 3544 forwarding unless you are using Teredo-based tunneling

IPv6 ACL to protect management access on VTY

- ipv6 access-list mgmt-vty
  - remark permit mgmt to local net only
  - permit ipv6 2001:db8:0:1::/64 any
- line vty 0 4
  - ipv6 access-class mgmt-vty in

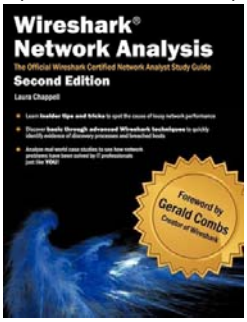
❖*Example for Cisco IOS*

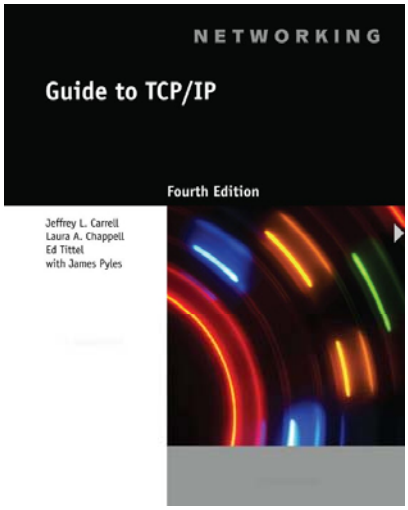
IPv6 Attack tools

- 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

Resources

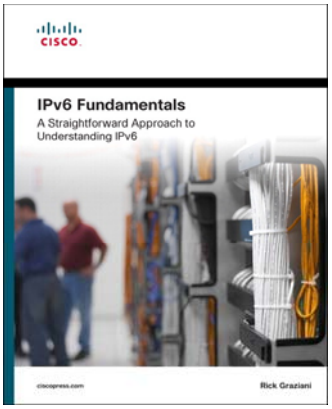
- Guide to TCP/IP, 4th Edition (Published September 2012)
- Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide (Published March 2012)



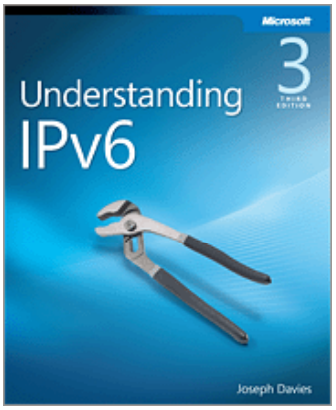


Resources

- IPv6 Fundamentals
  (Published October 2012)

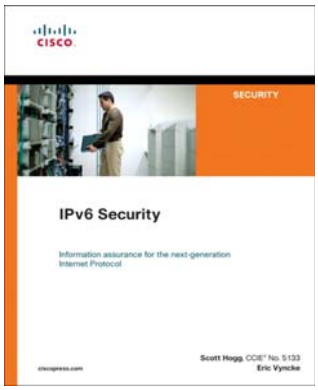


- Understanding IPv6, 3rd Edition
  (Published June 2012)

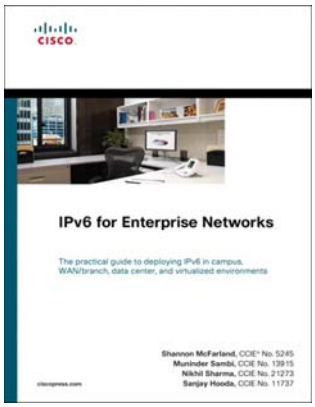


Resources

- IPv6 Security
  (Published December 2008)

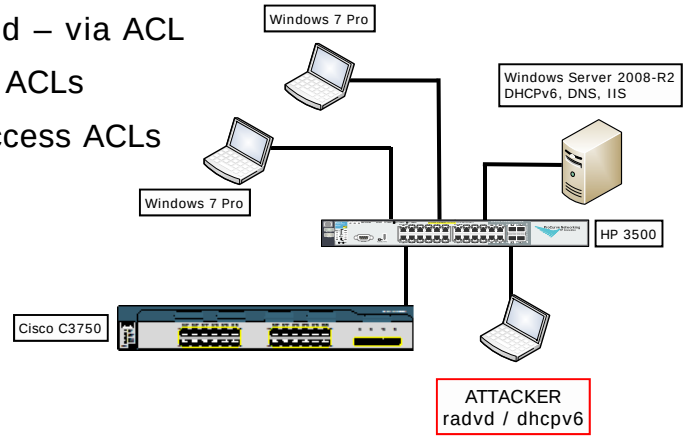


- IPv6 for Enterprise Networks
  (Published April 2011)



IPv6 FHS mitigation demonstration

- RA-Guard
- RA-Guard – via ACL
- DHCPv6 ACLs
- Mgmt access ACLs



Thank You for Attending!

Jeffrey L Carrell
Network Security Consultant
jeff.carrell@networkconversions.com