IPv6 Infrastructure Security
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

- Company ID
- Manufacturer Data

```
00 19 71 64 3F 00
```

- IEEE 48-Bit MAC Address
- Expand to EUI-64
- Invert the Global Bit
- Modified EUI-64 Interface ID

```
02 19 71 FF FE 64 3F 00
```

```
0219:71FF:FE64:3F00
```
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
- 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 (aka 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

<table>
<thead>
<tr>
<th>Address Autoconfiguration Method</th>
<th>ICMPv6 RA (Type 134) Flags</th>
<th>ICMPv6 RA (Type 134) M Flag</th>
<th>ICMPv6 Option Prefix Info A Flag</th>
<th>Prefix Derived from</th>
<th>Interface ID Derived from</th>
<th>Other Configuration Options (DNS, time, TFTP, etc)</th>
<th>Number of IPv6 Addresses on</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local (always configured)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Internal (fe80::/64)</td>
<td>M-EUI-64 or Privacy</td>
<td>Manual</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>SLAAC</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>RA</td>
<td>M-EUI-64 or Privacy</td>
<td>3</td>
<td>(LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Stateful (DHCPv6)</td>
<td>On</td>
<td>N/R</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>DHCPv6</td>
<td>2</td>
<td>(LL, DHCPv6)</td>
</tr>
<tr>
<td>Stateless DHCPv6</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>RA and DHCPv6</td>
<td>3</td>
<td>(LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Combination Stateless &amp; DHCPv6</td>
<td>On</td>
<td>N/R</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>RA and DHCPv6</td>
<td>4</td>
<td>(LL, IPv6, IPv6 temp, DHCPv6)</td>
</tr>
</tbody>
</table>
Router Advertisement packet

IPv6 autoconfiguration options

<table>
<thead>
<tr>
<th>Address Autoconfiguration Method</th>
<th>ICMPv6 RA (Type 133)</th>
<th>ICMPv6 RA (Type 134)</th>
<th>ICMPv6 Option Prefix Info</th>
<th>Prefix Derived from</th>
<th>Interface ID Derived from</th>
<th>Other Configuration Options (DNS, time, tftp, etc)</th>
<th>Number of IPv6 Addresses on Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-local</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Internal (Link-local)</td>
<td>Manual</td>
<td>1</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>RA</td>
<td>M-EUI-64 or Privacy</td>
<td>3 (LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Stateful (DHCPv6)</td>
<td>On</td>
<td>N/R</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>DHCPv6</td>
<td>2 (LL, DHCPv6)</td>
</tr>
<tr>
<td>Stateless DHCPv6</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>RA</td>
<td>M-EUI-64 or Privacy</td>
<td>3 (LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Combination Stateless &amp; DHCPv6</td>
<td>On</td>
<td>N/R</td>
<td>On</td>
<td>On</td>
<td>RA and DHCPv6</td>
<td>M-EUI-64 or Privacy</td>
<td>4 (LL, IPv6, IPv6 temp, DHCPv6)</td>
</tr>
</tbody>
</table>
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 autoconfiguration options

<table>
<thead>
<tr>
<th>Address Autoconfiguration Method</th>
<th>ICMPv6 RA (Type 134)</th>
<th>ICMPv6 RA (Type 134)</th>
<th>Prefix Derived from</th>
<th>Interface ID Derived from</th>
<th>Other Configuration Options (DNS, time, TCP, etc)</th>
<th>Number of IPv6 Addresses on Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local (always configured)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Manual</td>
<td>1</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>RA M-EUI-64 or Privacy</td>
<td>3 (LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Stateful (DHCPv6)</td>
<td>On</td>
<td>N/R</td>
<td>Off</td>
<td>On</td>
<td>DHCPv6</td>
<td>2 (LL, DHCPv6)</td>
</tr>
<tr>
<td>Stateless DHCPv6</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>RA M-EUI-64 or Privacy</td>
<td>3 (LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Combination Stateless &amp; DHCPv6</td>
<td>On</td>
<td>N/R</td>
<td>On</td>
<td>On</td>
<td>RA M-EUI-64 or Privacy and DHCPv6</td>
<td>4 (LL, IPv6, IPv6 temp, DHCPv6)</td>
</tr>
</tbody>
</table>
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 autoconfiguration options

<table>
<thead>
<tr>
<th>Address Autoconfiguration Method</th>
<th>ICMPv6 RA (Type 134) Flags</th>
<th>Prefix Info Derived from</th>
<th>Other Configuration Options (DNS, time, tftp, etc.)</th>
<th>Number of IPv6 Addresses on Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local (always configured)</td>
<td>N/A</td>
<td>N/A</td>
<td>M-EUI-64 or Privacy</td>
<td>1</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Off</td>
<td>On</td>
<td>RA M-EUI-64 or Privacy</td>
<td>3</td>
</tr>
<tr>
<td>Stateful (DHCPv6)</td>
<td>On</td>
<td>N/R</td>
<td>DHCPv6</td>
<td></td>
</tr>
<tr>
<td>Stateless DHCPv6</td>
<td>Off</td>
<td>On</td>
<td>RA M-EUI-64 or Privacy</td>
<td>3</td>
</tr>
<tr>
<td>Combination Stateless &amp; DHCPv6</td>
<td>On</td>
<td>N/R</td>
<td>RA and DHCPv6</td>
<td></td>
</tr>
</tbody>
</table>

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
IPv6 Stateful (DHCPv6) process

- DHCPv6Solicit = DHCPDistribute (IPv4)
- DHCPv6Advertise = DHCPOffer (IPv4)
- DHCPv6Request = DHCPRequest (IPv4)
- DHCPv6Reply = DHCPAck (IPv4)

Router Advertisement packet (Stateful/DHCPv6)
W2K8-R2 DHCPv6 server operation

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 !)
DHCPv6 Unique Identifier - DUID

- Each DHCP client and server has a DUID
- DHCP servers use DUIDs to identify clients for the selection of configuration parameters and in the association of IAs with clients
- DHCP clients use DUIDs to identify a server in messages where a server needs to be identified

(ref RFC 3315)

Cloning clients and DUID

- When a client machine is cloned, all the clones have the same DUID
- When 2 clients with the same DUID request an IPv6 address, the DHCPv6 server provides the same address to both clients
- When the 2nd client performs DAD, it detects an IPv6 address conflict, and will not go “on link”
Cloning clients and DUID

- For cloned MS Windows clients, the DUID is in the Windows Registry and can be removed with a manual operation (regedit)
- This should be done before creating a clone, so that when the clones are booted, new and unique DUIDs will be created
- reg deleteHKLMSYSTEMCurrentControlSetServicesTcpip6ParametersDhcpv6DUID

IPv6 autoconfiguration options

<table>
<thead>
<tr>
<th>Address Autoconfiguration Method</th>
<th>ICMPv6 RA (Type 133)</th>
<th>ICMPv6 RA (Type 134)</th>
<th>Prefix Derived from</th>
<th>Interface ID Derived from</th>
<th>Other Configuration Options (DNS, time, tftp, etc)</th>
<th>Number of IPv6 Addresses on Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local (always configured)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Internal (100/64)</td>
<td>M-EUI-64 or Privacy</td>
<td>1</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>On</td>
<td>M-EUI-64 or Privacy</td>
<td>3 (LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Stateful (DHCPv6)</td>
<td>On</td>
<td>N/R</td>
<td>Off</td>
<td>On</td>
<td>RA</td>
<td>2 (LL, DHCPv6)</td>
</tr>
<tr>
<td>Stateless DHCPv6</td>
<td>Off</td>
<td>On</td>
<td>On</td>
<td>On</td>
<td>RA</td>
<td>3 (LL, IPv6, IPv6 temp)</td>
</tr>
<tr>
<td>Combination Stateless &amp; DHCPv6</td>
<td>On</td>
<td>N/R</td>
<td>On</td>
<td>On</td>
<td>RA and DHCPv6</td>
<td>DHCPv6</td>
</tr>
</tbody>
</table>
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)

IPv6 addresses on Win7 client

Ethernet adapter Local Area Connection:

- Description: 169.254.0.0 to Fast Ethernet Adapter
- Physical Address: 00-16-55-61-16-FF
- DHCP Enabled: Yes
- Automatic Configuration Enabled: Yes
- IPv4 Address: 2001:db8:1a:1286:34e::63:1ksic(PREFERRED)
- Temporary IPv6 Address: 2001:db8:1a:1286:34e::63:1ksic(PREFERRED)
- Link-local IPv6 Address: fe80::63:1ksicle2ipa%(Preferred)
- IPv4 Address: 10.1.0.1(PREFERRED)
- Subnet Mask: 255.255.255.0
- Lease Obtained: Wednesday, April 04, 2012 4:08:27 PM
- Lease Expires: Thursday, April 05, 2012 3:59:00 AM
- Default Gateway: 10.1.0.1
- DHCP Server: 10.1.0.200
- DNS IPv6: 4026::7970
- DNS Client DUID: 80-01-08-01-15-08-74-0E-B8-2A-82-38-A7-5D
- DNS Server: 2001:db8:1ab:0a0:200A
- Nodisoverd: 10.1.0.200
- Nodiscovery: Enabled
- Connection-specific DNS Suffix Search List: iuphsanbox.com
IPv6 addresses on Mac Lion client

```
conf -L en0
en0: flags=8863<UP,BROADCAST,SMART, RUNNING, SIMPLEX, MULTICAST> mtu 1500
   options=2b:rscsum,txcsum, vlan, htagging, tsdu
ethernet 00:bc:80:cb:08:16/93
inet6 fe80::cc8b:8fff:fe00:1693/64 scopeid 0x4
inet 169.254.161.176/24 broadcast 169.254.255.255
inet6 fe80::cc8b:8ff:fe00:1693/64 scopeid 0x4
inet 2001:db8:1ab:ba5e::1/64
inet 2001:db8:1ab:ba5e::1/64
inet6 2001:db8:1ab:ba5e::1/64
inet6 2001:db8:1ab:ba5e::1/64
inet6 2001:db8:1ab:ba5e::1/64
```

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
```
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

IPv6 demonstration
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 it 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

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

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

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>DHCPv6 Snooping</th>
<th>ND Snooping</th>
<th>IPv6 Source Guard</th>
<th>RA-Guard (RFC6105)</th>
<th>SeND (RFC3971)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP – Comware 5</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (ND Detection)</td>
<td>No</td>
</tr>
<tr>
<td>(former 3Com/H3C)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP – ProVision ASIC</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>platforms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco IOS 12.2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(older 3560/3750)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco IOS 15.x</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(newer 3750E)</td>
<td>(DHCPv6 Guard)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Juniper JUNOS</td>
<td>&lt;future&gt;</td>
<td>&lt;future&gt;</td>
<td>&lt;future&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(EX series)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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 a widely implemented feature as of yet*

*Can be circumvented by modifying IPv6 Extension Headers*

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

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
IPv6 ACL - protect mgmt 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!
  - SI6 Networks IPv6 Toolkit – 2 dozen tools!

- Scanners
  - Nmap, halfscan6 (older)

- Packet forge
  - Scapy

- DoS Tools (older)
  - 6tunneldos, 4to6ddos, Imps6-tools
Resources

- Guide to TCP/IP, 4th Edition  
  (Published September 2012)

  (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
- DHCPv6 ACL

Diagram:
- Windows 7 Pro
- Windows Server 2008 R2
- Cisco C3750
- HP 3500
- ATTACKER
  radvd / dhcpv6

Windows 7 Pro

Windows 7 Pro

Windows 7 Pro

Windows 7 Pro

Windows 7 Pro

Windows Server 2008 R2

DHCPv6, DNS, IIS

HP 3500

ATTACKER
radvd / dhcpv6
Thank You for Attending!

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