IPV6 ATTACKS AND COUNTERMEASURES

CDW Advanced Technology Services

James Small, Principal Network/Security Consultant

PROBLEMATIC APPROACHES TO IPV6

If I ignore it, nothing will happen…

Image Source: wordpress.com

If I deploy it, I'll get DoS'ed!

Image Source: thethingaboutflying.com

IPV6 "PROBLEMS" WE'LL PUT TO REST

- VPN Bypass
- Router Advertisement Spoofing/Flooding
- DHCPv6 Spoofing
- Remote Scanning/DoS Attack
- Monitoring and Detection
- Preventing Tunneling and Firewalling
- Loss of NAT "Security"

Q&A throughout, I may postpone questions until the end depending on time

ROADMAP

- ***VPN Bypass***
- Router Advertisement Spoofing/Flooding
- DHCPv6 Spoofing
- Remote Scanning/DoS Attack
- Monitoring and Detection
- Preventing Tunneling and Firewalling
- Loss of NAT “Security”

VPN BYPASS

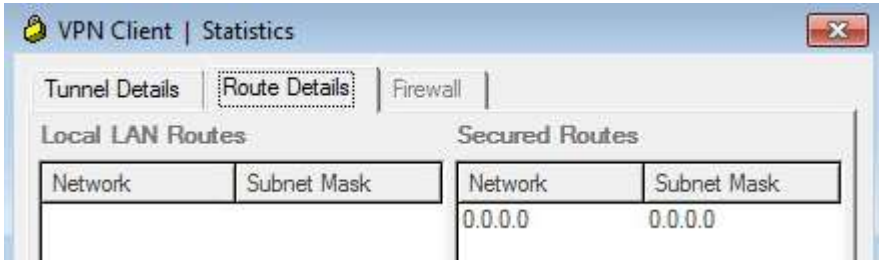
Many organizations allow remote user VPN access to their networks

- Often times access control and/or firewall policies are pushed to the client
  - » However, these policies are typically IPv4 only
- Many also disallow or restrict "split tunneling" – the ability to send network traffic without going through the VPN session

- One risk of allowing split-tunneling is that the remote user VPN client could be used as a bridgehead into the organizations network
  - » Remote user connects to organization via VPN
  - » Attacker compromises user system, goes from the Internet through the system into organization

VPN BYPASS

Belief: My VPN solution does not allow "split tunneling" – all traffic is forced through the VPN:



Expected view of system traffic:

Source	Destination	Src Port	Dst Port	Protocol	Info
172.21.1.103	172.21.1.1	54842	500	ISAKMP	Transaction (Config Mode)
172.21.1.1	172.21.1.103	500	54842	ISAKMP	Transaction (Config Mode)
172.21.1.103	172.21.1.1	54842	500	ISAKMP	Transaction (Config Mode)
172.21.1.103	172.21.1.1	54842	500	ISAKMP	Transaction (Config Mode)
172.21.1.103	172.21.1.1	54842	500	ISAKMP	Quick Mode
172.21.1.1	172.21.1.103	500	54842	ISAKMP	Informational
172.21.1.1	172.21.1.103	500	54842	ISAKMP	Quick Mode
172.21.1.103	172.21.1.1	54842	500	ISAKMP	Quick Mode
00:0c:29:be:1a:8b	ff:ff:ff:ff:ff:ff			ARP	Who has 172.21.1.1? Tell 172.21.1.103
02:19:07:24:4f:cc	00:0c:29:be:1a:8b			ARP	172.21.1.1 is at 02:19:07:24:4f:cc
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.1	172.21.1.103			ESP	ESP (SPI=0x4d82aee7)
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.1	172.21.1.103			ESP	ESP (SPI=0x4d82aee7)
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)

VPN BYPASS

Reality: All IPv4 traffic is forced over the VPN, IPv6 traffic completely bypasses it

- If the system receives an IPv6 Router Advertisement it will immediately configure IPv6:
  - » This may include a global address, a default route, and a new DNS server
  - » This new IPv6 address, default route, and DNS server will be preferred over the IPv4 options (See RFC 6724/3484)
  - » Do you see anything concerning about this "full-tunnel" VPN client traffic:

Source	Destination	Src Port	Dst Port	Protocol	Info
172.21.1.103	172.21.1.1			ESP	ESP (SPI=0xcd180228)
172.21.1.1	172.21.1.103			ESP	ESP (SPI=0x4d82aee7)
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1670	80	TCP	netview-aix-10 > http [SYN] Seq=0
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1669	80	TCP	netview-aix-9 > http [SYN] Seq=0 W
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1670	TCP	http > netview-aix-10 [SYN, ACK] S
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1670	80	TCP	netview-aix-10 > http [ACK] Seq=1
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1670	80	HTTP	GET /complete/search?q=www.goog&cl
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1669	TCP	http > netview-aix-9 [SYN, ACK] Se
2001:470:c4e8:10:2c29:6796:	ord08s06-in-x0e.1e100.net	1669	80	TCP	netview-aix-9 > http [ACK] Seq=1 A
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1670	TCP	http > netview-aix-10 [ACK] Seq=1
ord08s06-in-x0e.1e100.net	2001:470:c4e8:10:2c29:6796:	80	1670	HTTP/XML	HTTP/1.1 200 OK

VPN BYPASS

Security challenges

- Accidental VPN Bypass – User has IPv6 at home or uses a dual stack network
  - » Is preventing split-tunneling important?
  - » Does the client's endpoint security protect against IPv6 attacks?

- Malicious VPN Bypass – Attacker injects Router Advertisement to configure IPv6 on user's computer
  - » With control of DNS and IPv6, the attacker can
    - sniff all client traffic
    - attempt Man-In-The-Middle attacks
    - impersonate servers/systems and capture presented user credentials (e.g. NTLM)
    - gain access into your organization's network

VPN BYPASS - REMEDIATION

Solution

- Typically the vendor's current VPN solution supports IPv6
- For this particular case, the vendor has had a solution since early 2010
- ***Test your solution!***
- Ideally a VPN solution allows:
  - » Full support for either IPv4, IPv6 or both
  - » Supports IPv6 over IPv4 and IPv4 over IPv6
  - » Allows blocking/disabling either IPv4 or IPv6
  - » Allows VPN bypass of either IPv4 or IPv6 (but only on purpose!)
  - » Allows application of ACLs for either IPv4 or IPv6
  - » Allows pushing firewall policy for either IPv4 or IPv6

See Appendix for issues with disabling IPv6

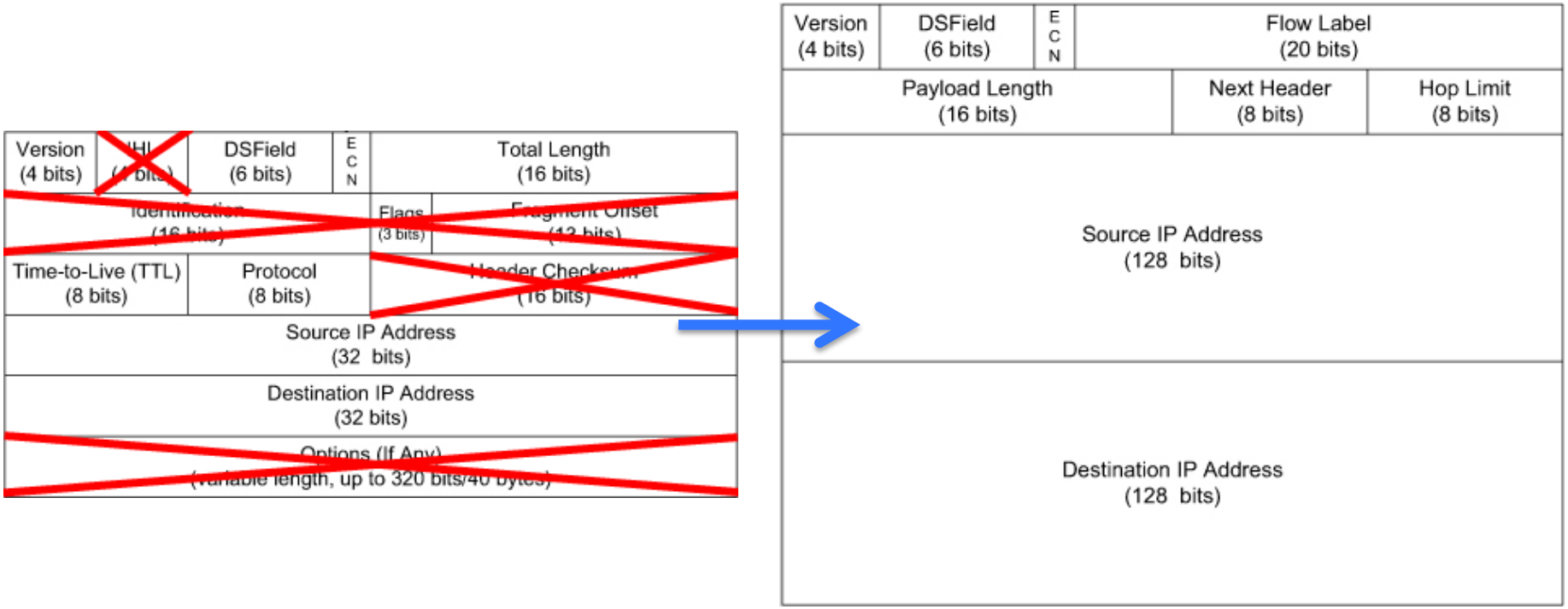
ROADMAP

- VPN Bypass
- ***Router Advertisement Spoofing/Flooding***
- DHCPv6 Spoofing
- Remote Scanning/DoS Attack
- Monitoring and Detection
- Preventing Tunneling and Firewalling
- Loss of NAT “Security”

IPV6 CHANGES – QUICK REFRESHER

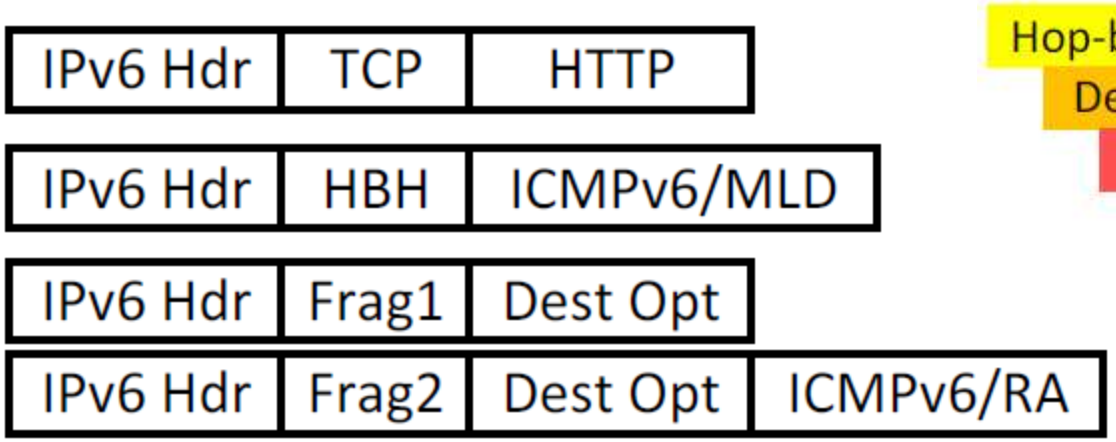
- Brief recap of the changes from IPv4 to IPv6
  - » In particular, fragmentation changes are important

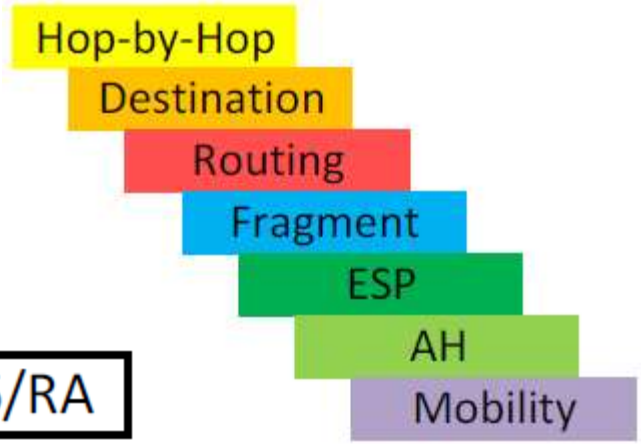
- As you know, IPv6 eliminates header options:
  - » Fixed length base header, fragmentation not handled here



IPV6 FRAGMENTATION

- Review – IPv6 header changes
  - » All options now Extension Headers including Fragmentation

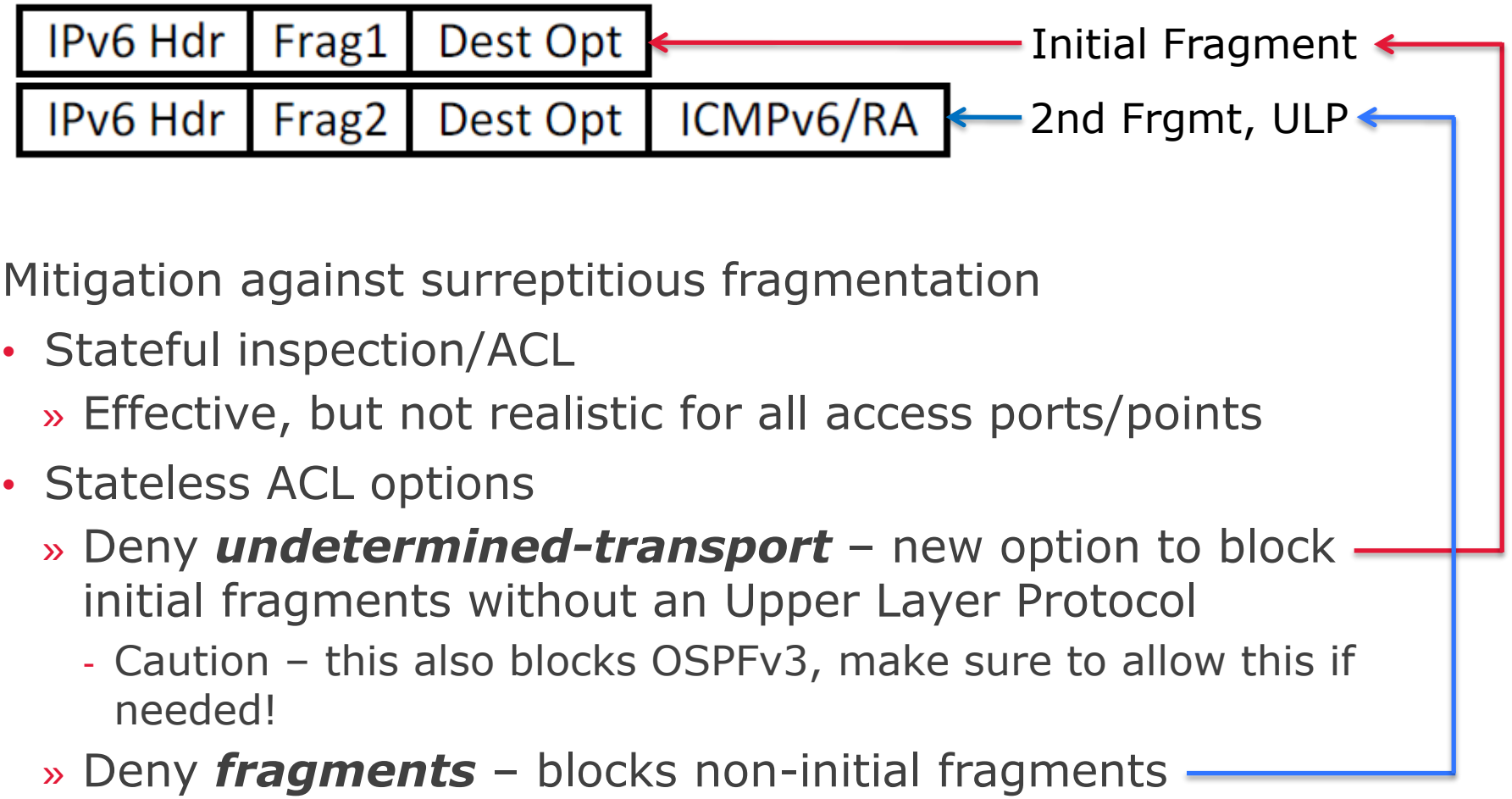




  - » Extension headers/Upper Layer Protocols are not required to be in the first packet
  - » If ULP not in first packet, stateless ACLs can be bypassed

IPV6 FRAGMENTATION CONTROLS

What if the IPv6 Upper Layer Protocol isn't in first packet?



Mitigation against surreptitious fragmentation

- Stateful inspection/ACL
  - » Effective, but not realistic for all access ports/points
- Stateless ACL options
  - » Deny ***undetermined-transport*** – new option to block initial fragments without an Upper Layer Protocol
    - Caution – this also blocks OSPFv3, make sure to allow this if needed!
  - » Deny ***fragments*** – blocks non-initial fragments

ROUTER ADVERTISEMENTS

- By default, Windows Vista and newer, OS X, and Linux have IPv6 enabled
- Many networks are only designed for IPv4 with no controls for IPv6
- What happens when an IPv6 enabled system receives a router advertisement?

Source	Destination	Src Port	Dst Port	Protocol	Info
fe80::d0:2bff:feff:74e5	ff02::1			ICMPv6	Router Advertisement from 02:d0:2b:ff:74:e5
fe80::7510:53ca:acda:2b04	ff02::1:ffff:74e5			ICMPv6	Neighbor Solicitation for fe80::d0:2bff:fef
fe80::d0:2bff:feff:74e5	fe80::7510:53ca:acda:2b04			ICMPv6	Neighbor Advertisement fe80::d0:2bff:feff:7
fe80::7510:53ca:acda:2b04	ff02::1:2	546	547	DHCPv6	Information-request XID: 0xd13192 CID: 0001
fe80::d0:2bff:feff:74e5	fe80::7510:53ca:acda:2b04	547	546	DHCPv6	Reply XID: 0xd13192 CID: 000100011699d2db00
fe80::7510:53ca:acda:2b04	ff02::16			ICMPv6	Multicast Listener Report Message v2
::	ff02::1:ffda:2b04			ICMPv6	Neighbor Solicitation for 2001:470:c4e8:10:
::	ff02::1:ff88:8a87			ICMPv6	Neighbor Solicitation for 2001:470:c4e8:10:
2001:470:c4e8:10:310a:b05e:	2001:470:c4e8:1:20c:29ff:fe	58202	53	DNS	Standard query 0x28ec A ipv6.msftncsi.com
2001:470:c4e8:1:20c:29ff:fe	2001:470:c4e8:10:310a:b05e:	53	58202	DNS	Standard query response 0x28ec CNAME ipv6.
2001:470:c4e8:10:310a:b05e:	2001:470:c4e8:1:20c:29ff:fe	49692	53	DNS	Standard query 0x70e4 AAAA ipv6.msftncsi.c
2001:470:c4e8:1:20c:29ff:fe	2001:470:c4e8:10:310a:b05e:	53	49692	DNS	Standard query response 0x70e4 CNAME ipv6.
2001:470:c4e8:10:310a:b05e:	a978.i6g1.akamai.net	1540	80	TCP	rds > http [SYN] Seq=0 Win=8192 Len=0 MSS=1
a978.i6g1.akamai.net	2001:470:c4e8:10:310a:b05e:	80	1540	TCP	http > rds [SYN, ACK] Seq=0 Ack=1 Win=14400
2001:470:c4e8:10:310a:b05e:	a978.i6g1.akamai.net	1540	80	TCP	rds > http [ACK] Seq=1 Ack=1 Win=66048 Len=
2001:470:c4e8:10:310a:b05e:	a978.i6g1.akamai.net	1540	80	HTTP	GET /ncsi.txt HTTP/1.1
a978.i6g1.akamai.net	2001:470:c4e8:10:310a:b05e:	80	1540	TCP	http > rds [ACK] Seq=1 Ack=99 Win=14400 Len
a978.i6g1.akamai.net	2001:470:c4e8:10:310a:b05e:	80	1540	HTTP	HTTP/1.1 200 OK (text/plain)

ROGUE ROUTER ADVERTISEMENTS (RA)

Security challenges

- Accidental RA
  - » User with Windows Internet Connection Sharing service enabled (think BYOD or power user)
  - » Someone connects a device configured for IPv6 routing to the network

- Malicious RA
  - » Attacker injects to attack network nodes as described in VPN Bypass section
  - » Attacker uses to flood the network as Denial of Service (DoS) attack

ROGUE RA MITIGATION – FIRST TRY

- Block RAs on unauthorized ports
  - RA Guard *(If available)*

```
ipv6 nd raguard policy HOST
 device-role host
!
vlan configuration 101
 ipv6 nd raguard attach-policy HOST
```

  - ACL:

```
ipv6 access-list HOST_PORT
 remark Block RAs on Host Ports
 deny icmp any any  router-advertisement
 permit ipv6 any any
!
interface GigabitEthernet0/1
 description Host Port
 ipv6 traffic-filter HOST_PORT in
```

ROGUE RA MITIGATION – FIRST TRY

- Does RA Guard or an IPv6 ACL work?
  - » Yes for non-malicious RAs
    - Test Windows 7 Workstation with Router on same VLAN
    - Router connected to switchport with ACL or RA Guard on VLAN
    - Router continuously generates RAs:

Source	Destination	Src Port	Dst Port	Protocol	Info
fe80::d0:2bff:feff:74e5	ff02::1			ICMPv6	Router Advertisement from 02:d0:2b:ff:74:e5
fe80::d0:2bff:feff:74e5	ff02::1			ICMPv6	Router Advertisement from 02:d0:2b:ff:74:e5
fe80::d0:2bff:feff:74e5	ff02::1			ICMPv6	Router Advertisement from 02:d0:2b:ff:74:e5
fe80::d0:2bff:feff:74e5	ff02::1			ICMPv6	Router Advertisement from 02:d0:2b:ff:74:e5

    - Check Workstation – No routable IPv6 address!

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter LAN:

   Connection-specific DNS Suffix  . : labnet.test
   Link-local IPv6 Address . . . . . : fe80::7510:53ca:acda:2b04%10
   IPv4 Address. . . . . . . . . . . : 172.21.1.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.21.1.1
```

ROGUE RA MITIGATION – FIRST TRY

- Does RA Guard or an IPv6 ACL work?
  - » What about malicious RAs?
    - Same Windows 7 Workstation with Linux Workstation on same VLAN
    - Linux Workstation connected to switchport with ACL or RA Guard on VLAN
      - RA generated by SI6 Networks' IPv6 Toolkit (ra6)

Source	Destination	Src Port	Dst Port	Protocol	Info
fe80::6a7f:74ff:feaf:244c	ff02::1			IPv6	IPv6 fragment (nxt=IPv6 destination option (60) off=0
fe80::6a7f:74ff:feaf:244c	ff02::1			ICMPv6	Router Advertisement from 68:7f:74:af:24:4c

    - Check Workstation – Uh oh…

```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter LAN:

   Connection-specific DNS Suffix  . : labnet.test
   IPv6 Address. . . . . . . . . . . : 2001:db8:1:2:7510:53ca:acda:2b04
   Temporary IPv6 Address. . . . . . : 2001:db8:1:2:f156:6cde:4884:c284
   Link-local IPv6 Address . . . . . : fe80::7510:53ca:acda:2b04%10
   IPv4 Address. . . . . . . . . . . : 172.21.1.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::6a7f:74ff:feaf:244c%10
                                       172.21.1.1
```

ROGUE RA CONTROLS – SECOND TRY, A

- How were the ACLs and RA Guard evaded?
  - » The fragmentation trick we showed earlier!
- ACL Mitigation (Using previously shown options)
  - » Use the undetermined-transport option *(If available)*
    - I went to try this out on my Cisco 3k access switch:

```
c3560cs(config)#ipv6 access-list HOST_PORT
c3560cs(config-ipv6-acl)#deny icmp any any router-advertisement
c3560cs(config-ipv6-acl)#deny ipv6 any any undetermined-transport
c3560cs(config-ipv6-acl)#permit ipv6 any any
c3560cs(config-ipv6-acl)#
c3560cs(config-ipv6-acl)#interface g0/8
c3560cs(config-if)#ipv6 traffic-filter HOST_PORT in
% This ACL contains following unsupported entries.
% Remove those entries and try again.
    deny ipv6 any any undetermined-transport sequence 20
% This ACL can not be attached to the interface.
c3560cs(config-if)#
Apr 18 23:13:30.400 EDT: %PARSE_RC-4-PRC_NON_COMPLIANCE: `ipv6 traffic-filter HOST_PORT in'
c3560cs(config-if)#
```

    - Then I discovered in the 2k/3k access switch configuration guide: ☹
      - The switch does not support matching on these keywords: flowlabel, routing header, and undetermined-transport.

ROGUE RA CONTROLS – SECOND TRY, B

Mitigation against fragmented rogue RAs continued:

- ACLs using the fragments option
  - » Drawback is what to block – a little more work
  - » Is blocking packets to ff02::1 sufficient? Unfortunately no.
  - » Sending RA to any multicast group the host is listening to or its link-local address activates IPv6 – must block them all

- Windows:

```
C:\>netsh int ipv6 show join

Interface 1: Loopback Pseudo-Interface 1

Scope       References  Last   Address
----------  ----------  ----   ------------------
0                    3  Yes    ff02::c

Interface 10: LAN

Scope       References  Last   Address
----------  ----------  ----   ------------------
0                    0  Yes    ff01::1
0                    0  Yes    ff02::1
0                    3  Yes    ff02::c
0                    1  Yes    ff02::1:3
0                    1  Yes    ff02::1:ffda:2b04
```

- Linux:

```
root@ubuntu:~# ip -6 maddr show
1:      lo
        inet6 ff02::1
2:      eth0
        inet6 ff02::fb
        inet6 ff02::1:ff99:11a5
        inet6 ff02::1
```

ROGUE RA CONTROLS – SECOND TRY, B

Mitigation against fragmented rogue RAs continued:

- ACLs using the fragments option
  - » Multicast/Link-local block candidates:
    - →Most dangerous←
    - ff02::1 (all nodes on link)
    - ff02::c (SSDP – Windows)
    - ff02::fb (MDNS – OS X, Linux)
    - ff02::1:3 (LLMNR – Windows)
    - →Harder to attack but possible←
    - ff02::1:ff00:0/104 (Solicited Node Multicast)
    - fe80::/64 (all link-local addresses)
    - →Unlikely, only configure if in use←
    - fe80::/10 (defined link-local – only fe80::/64 should be used but some systems allow)
    - ff02::/16 (all link-local multicast, also ff[137]2::/16)

ROGUE RA MITIGATION – SECOND TRY, B

Mitigation against fragmented rogue RAs continued:

- ACLs using the fragments option
  - » Reasonable ACL for most cases:

```
c3560cs(config)#ipv6 access-list HOST_PORT
c3560cs(config-ipv6-acl)#deny icmp any any  router-advertisement
c3560cs(config-ipv6-acl)#deny ipv6 any host FF02::1 fragments
c3560cs(config-ipv6-acl)#deny ipv6 any host FF02::C fragments
c3560cs(config-ipv6-acl)#deny ipv6 any host FF02::FB fragments
c3560cs(config-ipv6-acl)#deny ipv6 any host FF02::1:3 fragments
c3560cs(config-ipv6-acl)#deny ipv6 any FF02::1:FF00:0/104 fragments
c3560cs(config-ipv6-acl)#deny ipv6 any FE80::/64 fragments
c3560cs(config-ipv6-acl)#permit ipv6 any any
c3560cs(config-ipv6-acl)#
c3560cs(config-ipv6-acl)#interface g0/8
c3560cs(config-if)#ipv6 traffic-filter HOST_PORT in
```

- Of course, if your nodes listen on other IPv6 multicast groups you have to add those too

ROGUE RA MITIGATION – THE END?

While discussing this with Enno Rey he pointed out that actually the undetermined-transport option does work!

- Documentation/Error messages – bah!
- A few options:
  - » Apply the PACL to the port without the undetermined-transport ACE
  - » After the PACL is applied then add the option…and it works!
- Or:
  - » Add an empty PACL to the port
  - » Then create the ACL entries:

```
c3560cs(config)#interface g0/8
c3560cs(config-if)#ipv6 traffic-filter HOST_PORT in
c3560cs(config-if)#
c3560cs(config-if)#ipv6 access-list HOST_PORT
c3560cs(config-ipv6-acl)#deny icmp any any  router-advertisement
c3560cs(config-ipv6-acl)#deny ipv6 any any undetermined-transport
c3560cs(config-ipv6-acl)#permit ipv6 any any
```

ROGUE RA MITIGATION – THE END?

- Caveats
  - » If you want to apply it to other ports you have to remove the undetermined-transport option and add it back
  - » Reboots do not seem to be a problem but there may be other quirks
  - » May not be supported by Cisco TAC

RA FLOODING

One Denial of Service attack that gets repeated press is router advertisement flooding

- A system connected to your LAN can flood RAs causing a DoS for many systems including:
  - 100% CPU Utilization
  - Hanging/Crashing/Rebooting

- But…
  - Only works against systems on same LAN (L2 adjacent)
  - Typically requires high speed network with quality switch (won't work with something from Best Buy!)
  - Generally doesn't work over Wireless
  - Requires some work and only a DoS, can't exploit so better attacks available

RA FLOODING – TEST SETUP

Tools:

- The Hackers Choice, thc-ipv6 suite (attack/fuzzing tools)
  - fake_router6, flood_router26
- SI6 Networks IPv6 Toolkit (really meant for fuzzing/hardening)
  - ra6

Tested Attacks with:

- Quad-core i7 high end laptop that generates 120,000 pps
  - Running Ubuntu 12.10
- Cisco 3000 series gigabit switch (C/E/X-Series)
  - IP Base, 15.0(2)SE
  - RA Guard (as shown previously)
  - IPv6 ACLs (as shown previously)

RA FLOODING - OVERVIEW

In a pristine lab environment:

- Use fake_router6 and flood_router26
  - » flood_router26 generates 17 prefixes and 17 routes per RA
  - » Sends them as fast as possible to overwhelm host

```
Ethernet II, Src: WistronI_59:61:8b (3c:97:0e:59:61:8b), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::76:a3e9:7636:3901 (fe80::76:a3e9:7636:3901), Dst: ff02::1 (ff02::1)
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0x0fff [correct]
  Cur hop limit: 255
⊞ Flags: 0x08
  Router lifetime (s): 65535
  Reachable time (ms): 16384000
  Retrans timer (ms): 1966080
⊞ ICMPv6 Option (MTU : 1500)
⊞ ICMPv6 Option (Source link-layer address : 00:0c:e9:76:36:39)
⊞ ICMPv6 Option (Prefix information : 2012:76a4:ea76:3639::/64)
⊞ ICMPv6 Option (Prefix information : 2012:76a5:ec76:3639::/64)
⊞ ICMPv6 Option (Prefix information : 2012:76a6:ee76:3639::/64)
⊞ ICMPv6 Option (Prefix information : 2012:76a7:f076:3639::/64)
```

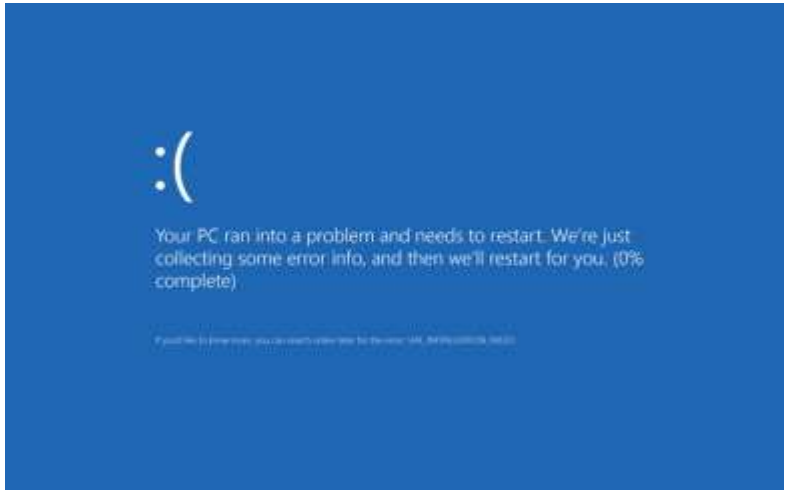
(Lots of Prefix/Route Information options omitted…)

```
⊞ ICMPv6 Option (Route Information : High 2004:76be:fd76:3639::/64)
⊞ ICMPv6 Option (Route Information : High 2004:76bf:ff76:3639::/64)
⊞ ICMPv6 Option (Route Information : High 2004:76c0:177:3639::/64)
⊞ ICMPv6 Option (Route Information : High 2004:76c1:377:3639::/64)
⊞ ICMPv6 Option (Route Information : High 2004:76c2:577:3639::/64)
```

RA FLOODING - RESULTS

Test 1 – no defenses

- Use fake_router6 and flood_router26, no options
- Windows 7 (with KB2750841) unusable when flooded but recovers quickly when flood ends
- Windows Vista becomes unusable, sometimes crashes
- Windows 8 Crashes



RA FLOODING - RESULTS

Test 2 – use RA Guard

- Use fake_router6 and flood_router26
  - » Blocks with no options but…
  - » Can bypass RA Guard with –D (uses fragmentation tactics described earlier)
  - » However:
    - With a blazing fast laptop attacking I still couldn't crash Windows 8 or Vista and none of the systems were unresponsive
    - But does trash IPv6 configuration – all IPv6 addresses/routes are overwritten
- Using SI6 Networks ra6
  - » With carefully crafted fragmented packets it is still possible to crash Windows 8 and Vista, but hard and not consistent
  - » 7 is as before – worst you can do is bog it down, but quickly recovers subsequent to attack

RA FLOODING - RESULTS

Test 3 – use IPv6 ACLs described previously (undetermined-transport/fragments)

- Use fake_router6, flood_router26, and ra6
  - » Some fragments (initial or subsequent) get through but are harmless
  - » No noticeable effect on the systems

- Bottom Line - Make sure to Test your Equipment!
  - » Older hardware/ASICs have limited or no support for these features – make sure to read the documentation and validate the configuration!

ROADMAP

- VPN Bypass
- Router Advertisement Spoofing/Flooding
- ***DHCPv6 Spoofing***
- Remote Scanning/DoS Attack
- Monitoring and Detection
- Preventing Tunneling and Firewalling
- Loss of NAT “Security”

DHCPV6 SPOOFING

- By default, some operating systems such as Windows (Vista and newer) try to configure IPv6 via DHCPv6 (even without RA!)

Source	Destination	Src Port	Dst Port	Protocol	Info
::	ff02::1:ff9f:7525			ICMPv6	Neighbor Solicitation for fe80::8021:aecd:e9f:7525
fe80::8021:aecd:e9f:7525	ff02::2			ICMPv6	Router Solicitation from 00:26:2d:fc:05:9b
fe80::b19f:e83d:2040:e303	ff02::1:2	546	547	DHCPv6	Solicit XID: 0xe6b308 CID: 0001000115265a61001bb1f2
fe80::8021:aecd:e9f:7525	ff02::2			ICMPv6	Router Solicitation from 00:26:2d:fc:05:9b
fe80::36c0:59ff:fe08:ee3e	ff02::2			ICMPv6	Router Solicitation from 34:c0:59:08:ee:3e
fe80::91f3:fe40:bbe0:c3ac	ff02::1:2	546	547	DHCPv6	Solicit XID: 0x47ac1f CID: 000100011054841500221 5ff
fe80::91f3:fe40:bbe0:c3ac	ff02::1:2	546	547	DHCPv6	Solicit XID: 0x47ac1f CID: 000100011054841500221 5ff
fe80::e2b9:baff:fedf:9bc7	ff02::2			ICMPv6	Router Solicitation from e0:b9:ba:df:9b:c7
fe80::8021:aecd:e9f:7525	ff02::2			ICMPv6	Router Solicitation from 00:26:2d:fc:05:9b

- The issues are similar as described for Router Advertisements
- What happens when an IPv6 enabled system receives a DHCPv6 response?
  - » It will configure an IPv6 address
  - » It will configure a DNS server
  - » It will configure a DNS search list
  - » Note: It won't configure any routes or a default gateway – these must come from RAs!

ROGUE DHCPV6 SERVER

Security challenges similar to RAs

- Accidental
  - » Someone connects a device configured for DHCPv6 to the network

- Malicious
  - » Attacker responds to a DHCPv6 request with spoofed information
  - » Notes:
    - Not as easy as spoofed RAs – attacker must respond to client requests with valid information making it easier to trace
    - Not as dangerous as rogue RAs, primary threat is attacker gaining control of DNS

ROGUE DHCPV6 MITIGATION – FIRST TRY

- Block DHCPv6 on unauthorized ports
  - DHCPv6 Guard

```
ipv6 dhcp guard policy CLIENT
 device-role client
!
vlan configuration 101
 ipv6 dhcp guard attach-policy CLIENT
```

  - ACL:

```
ipv6 access-list CLIENT_PORT
 remark Block DHCPv6 Server on Client Ports
 deny udp any eq 547 any
 permit ipv6 any any
!
interface GigabitEthernet0/1
 description Host Port
 ipv6 traffic-filter HOST_PORT in
```

ROGUE DHCPV6 MITIGATION – EFFICACY

- Does DHCPv6 Guard or an IPv6 ACL work?
  - » Yes for non-malicious/non-fragmented DHCPv6 packets

- As with RAs, DHCPv6 Guard and basic ACLs can be bypassed with the fragmentation evasion
  - » But – no known attack tools in the wild that have the fragmentation evasion built in
  - » However…scapy could be used to craft an attack, but would be some work

ROGUE DHCPV6 MITIGATION – SECOND TRY

Mitigation options against fragmented DHCPv6 replies:

- Option A – block fragment evasion packets (initial packet) with undetermined-transport option

- Option B – block fragment evasion packets (non-initial packets) with crafted ACL
  - » Unlike with RAs, DHCPv6 replies are unicast – easier to block
  - » DHCPv6 packets use a link-local address, so block fragments from:
    - fe80::/64 (all link-local addresses)

    →Unlikely, only configure if in use←
    - fe80::/10 (defined link-local – only fe80::/64 should be used but some systems allow)

ROGUE DHCPV6 MITIGATION – SECOND TRY

Mitigation options against fragmented DHCPv6 replies:

- Option A:

```
c3560cs(config)#ipv6 access-list CLIENT_PORT-OptA
c3560cs(config-ipv6-acl)#deny udp any eq 547 any
c3560cs(config-ipv6-acl)#deny ipv6 any any undetermined-transport
c3560cs(config-ipv6-acl)#permit ipv6 any any
c3560cs(config-ipv6-acl)#
c3560cs(config-ipv6-acl)#interface g0/8
c3560cs(config-if)#ipv6 traffic-filter CLIENT_PORT-OptA in
```

- Option B:

```
c3560cs(config)#ipv6 access-list CLIENT_PORT-OptB
c3560cs(config-ipv6-acl)#deny udp any eq 547 any
c3560cs(config-ipv6-acl)#deny ipv6 any fe80::/64 fragments
c3560cs(config-ipv6-acl)#permit ipv6 any any
c3560cs(config-ipv6-acl)#
c3560cs(config-ipv6-acl)#interface g0/8
c3560cs(config-if)#ipv6 traffic-filter CLIENT_PORT-OptB in
```

DHCPV6 FLOODING?

- An IPv6 subnet has over 18 quintillion addresses
- Try to use up all the leases is futile, attackers won't wait for years
- However, as with IPv4 you can limit the number of addresses leased per port with IPv6 snooping.

ROADMAP

- VPN Bypass
- Router Advertisement Spoofing/Flooding
- DHCPv6 Spoofing
- ***Remote Scanning/DoS Attack***
- Monitoring and Detection
- Preventing Tunneling and Firewalling
- Loss of NAT “Security”

REMOTE SCANNING DOS

- Attacker (aggressively) scans a network (e.g. scan6)
  - » Scan triggers neighbor discovery (resolve address to MAC)
  - » The theory is that the flood of NDP packets overwhelms the router/switch and thus a DoS

Issue?

- Local scan (attacker scanning same VLAN) could be:
  - » Not an IPv6 issue – excessive L2 broadcast/multicast traffic can overload some switches
  - » Solution – throttle broadcast/multicast traffic on host ports to reasonable levels, e.g.:
    - storm-control broadcast level 2.00 1.00
    - storm-control multicast level 5.00 1.00
  - » Also – Destination Guard (next topic!)

REMOTE SCANNING DOS

Issue?

- Remote scan:
  - » Does not generally appear to be an issue for Cisco devices

- IOS has a built in rate limiter (not tunable)
  - » show ipv6 traffic - look under ICMP statistics, Sent, # output, ***# rate-limited***
- IOS limits incomplete NDP entries
  - » show ipv6 neighbors statistics – INCMP appears to be capped at 512
- IOS appears to have separate caches for incomplete versus completed entries
- Newer versions of IOS allow NDP cache tuning if desired:
  - » ipv6 nd cache interface-limit #

REMOTE SCANNING DOS

But what if it could possibly be an issue?

Mitigations:

- Ingress ACLs
- Destination Guard – the silver bullet!

Destination Guard:

- Using IPv6 snooping/gleaning the switch learns all L2 neighbors
- When an attacker tries to scan a subnet the switch can:
  - » Summarily drop all requests for unknown neighbors
  - » Only drop requests for unknown neighbors under stress
- Cons? Only available on 4500s and 7600s today, but coming on other platforms.

ROADMAP

- VPN Bypass
- Router Advertisement Spoofing/Flooding
- DHCPv6 Spoofing/Flooding
- Remote Scanning/DoS Attack
- ***Monitoring and Detection***
- Preventing Tunneling and Firewalling
- Loss of NAT “Security”

MONITORING AND CONTROLLING IPV6

Service	Number	Description
IPv6 Encapsulation	IPv4/41	Tunnel IPv6 over IPv4
Generic Tunnel	IPv4/47	Tunnel anything over GRE
Teredo/Miredo	UDP/3544	Tunnel IPv6 over UDP (NAT Traversal)
Teredo/Miredo	Non-Standard	IPv6 destination starting with 2001:0000::/32 over UDP over IPv4
TSP	TCP|UDP/3653	IPv6 Tunnel Broker using the Tunnel Setup Protocol (RFC 5572)
AYIYA	TCP|UDP/5072	IPv6 Tunnel Broker using Anything in Anything (www.sixxs.net/tools/ayiya/)
Public 6to4 Anycast Relay	IPv4:192.88.99.1	Starting with IPv6 source address of 2002::/16 (6to4 is IPv6 over IPv4/41) Destined to 192.88.99.0/24 for IPv4
IPv6 Encapsulation	TCP/443	IPv6 over IPv4 SSL Tunnel, many variants
IPv6 Ethertype	0x86DD	Distinct from IPv4 Ethertype (0x0800)
DNS IPv6 Records	Several	AAAA, updated PTR records - can be transported over IPv4 or IPv6

Image source: gfi.com

ROADMAP

- VPN Bypass
- Router Advertisement Spoofing/Flooding
- DHCPv6 Spoofing/Flooding
- Remote Scanning/DoS Attack
- Monitoring and Detection
- ***Preventing Tunneling and Firewalling***
- Loss of NAT “Security”

EXAMPLE FIREWALL POLICY

Block Tunneling IPv6 through IPv4 network:

Source Criteria:			Destination Criteria:		Service	Action	…	…	…	Description
Source	…	…	Destination	…						
ing rules, 9 filtered rules)										
any			any		41	Deny				Protocol 41 (IPv6 over IPv4 - ISATAP, 6to4, 6rd, 6in4, 6over4)
any			192.88.99.0/24		ip	Deny				Public 6to4 Anycast block
any			any		gre	Deny				GRE
any			any		3544	Deny				Teredo/Miredo
any			any		3563	Deny				TSP
any			any		5072	Deny				AYIYA
any			any		ip	Permit				

If you don’t want IPv6 traffic going through a firewall then explicitly block it!

IPV6 ACCESS CONTROL

- Firewall Policy
  - » Don’t block all ICMPv6!!!
  - » Simple Examples for transit traffic, can get more granular:

Source Criteria:		Destination Criteria:		Service	Action
Source	... ...	Destination	...		
ming rules)					
any6		any6		IPv6-Ops packet-too-big parameter-problem time-exceeded unreachable	Permit

Source Criteria:		Destination Criteria:		Service	Action
Source	... ...	Destination	...		
ming rules)					
any4		any4		IPv4-Ops parameter-problem time-exceeded unreachable	Permit

  - » Reference NIST SP 800-119 (Section 3.5, Table 3-7)
  - » Reference RFC 4890 (Recommendations for Filtering ICMPv6 Messages in Firewalls)

IPV6 ACCESS CONTROL

- Router/Switch Policy
  - » Don’t block the NDP’s NS/NA functionality or you will break IPv6!

ipv6 access-list Example1

permit any host 2001:db8::1

permit icmp any any nd-ns

permit icmp any any nd-na

deny ipv6 any any

ROADMAP

- VPN Bypass
- Router Advertisement Spoofing/Flooding
- DHCPv6 Spoofing/Flooding
- Remote Scanning/DoS Attack
- Monitoring and Detection
- Preventing Tunneling and Firewalling
- ***Loss of NAT "Security"***

NAT SECURITY

NAT Security Considerations:

- Topology hiding
  - » Pros – Makes attacks more challenging
  - » Cons – Operational costs/complexity, impedes easy communication
- Prevents inbound access without prior outbound access
  - » Pros – Protection against a poorly configured firewall/ACL
  - » Cons – Same as above

General Security Considerations:

- Most security comes from stateful firewalls and application inspection
- Most attacks/compromises are “drive-bys” or the result of user initiated activities which NAT offers no protection against

WHY IPV6 AND NO NAT?

- Address space
  - » Should be a virtually unlimited supply – think street addresses
  - » Facilitates communication/collaboration

- Innovation
  - » NAT Gateways make innovation harder (mainly driven by insufficient address space)
  - » Productivity (easy communication/collaboration) is a key business objective which NAT impedes

PROBLEMS WITH NAT

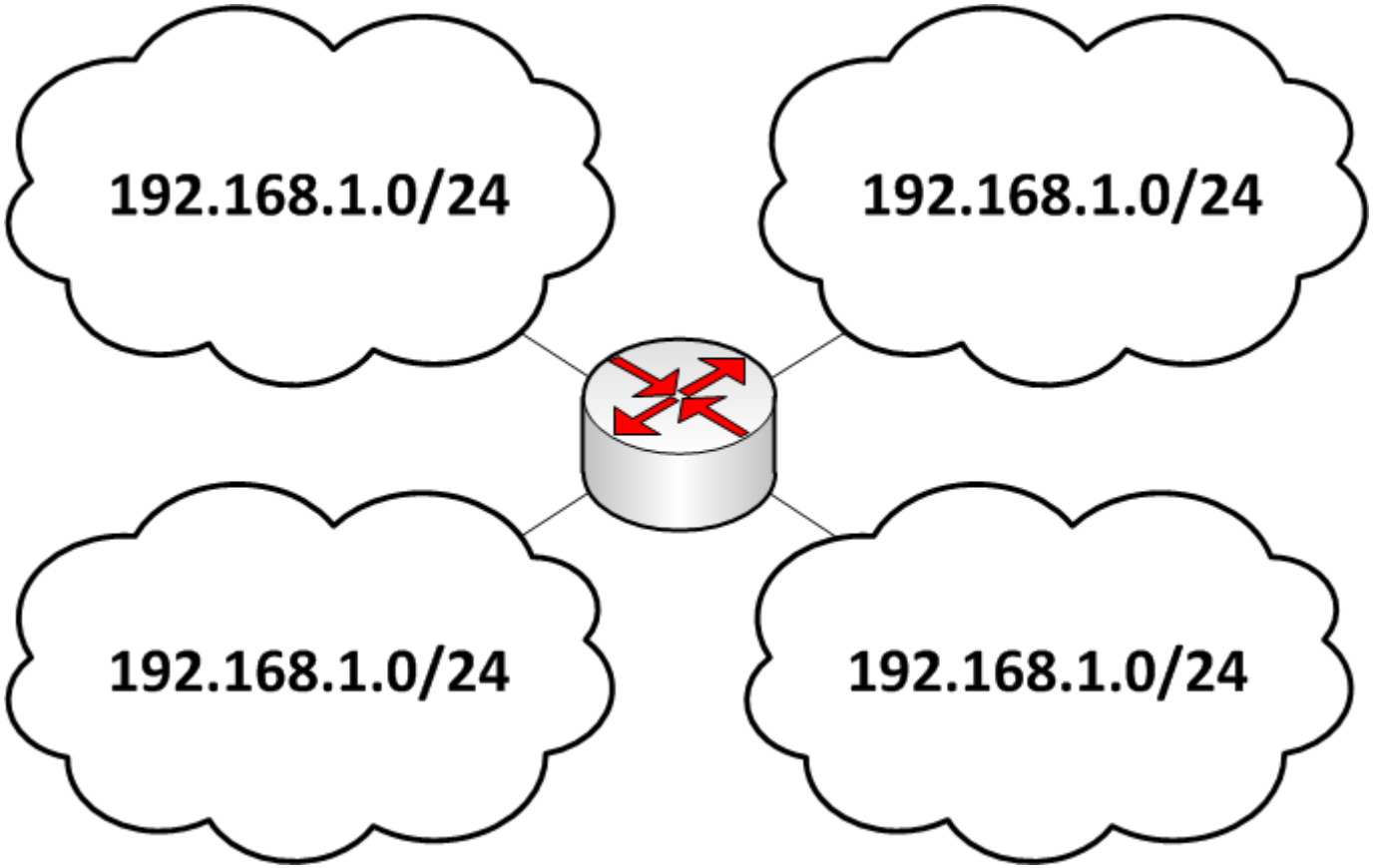
- Some protocols do not work correctly through NAT and require "fix-ups" (ALG's) or extra configuration
  - » E.g. ICMP, FTP, SIP, H.323, RTSP, some VPNs
- NAT breaks end-to-end connectivity
  - » Connection establishment and/or packet data requires a 3rd party
  - » Affects Voice Calls, Video Conferencing, file sharing, Collaboration, etc. For example, Skype, Facetime, Webex, and Microsoft Sharepoint Workspace work better without NAT.
  - » Note: Multiple NAT tiers can totally break these applications
- NAT for address overlap is technically challenging
- Limits innovation, increases costs/barriers for new ideas/solutions

BENEFITS OF NAT

- NAT simplifies changing ISPs (If PI Addresses not used)
- NAT hides the network topology and foils many simple network scans
  - » NAT alone is ***not*** secure, but it has been a helpful safety net against sloppy firewall policies
  - » Without NAT, firewall policies must be more robust and actively managed
- NAT can easily solve some complex network issues
  - » Multi-homing ISP's, return path selection, asymmetric routing
- NAT is ubiquitous
  - » Today, software is developed with an expectation of NAT
  - » Tomorrow…?

THE HIDDEN COSTS OF NAT

Something to consider when evaluating NAT:



QUESTIONS

CDW Advanced Technology Services

cdw.com/services

CDW Solutions Blog:
cdwsolutionsblog.com

BACKUP SLIDES

Appendix

IPV6 SECURITY COUNTERMEASURES

Common IPv6 L2 Security Issues and Options:

Issue	Solution
Spoofed/Illegitimate RAs	**RA Guard (or PACL)**
Spoofed NDP NA	**MLD Snooping, DHCPv6 Snooping, NDP Inspection, ~~SeND~~**
(Spoofed) Local NDP NS Flood	**NDP Inspection, NDP Cache Limits, CoPP**
(Spoofed) Remote NDP NS Flood	**Ingress ACL, CoPP, NDP Cache Limits**
(Spoofed) DAD Attack	**MLD Snooping, NDP Inspection**
(Spoofed) DHCPv6 Attack	**DHCPv6 Guard**
Spoofed/Illegitimate DHCPv6 Replies	**DHCPv6 Guard (or PACL)**

REDMOND'S STANCE

Per the Microsoft IPv6 FAQ:

"From Microsoft's perspective, IPv6 is a mandatory part of the Windows operating system and it is enabled and included in standard Windows service and application testing during the operating system development process. Because Windows was designed specifically with IPv6 present, Microsoft does not perform any testing to determine the effects of disabling IPv6. If IPv6 is disabled on Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008, or later versions, some components will not function. Moreover, applications that you might not think are using IPv6—such as Remote Assistance, HomeGroup, DirectAccess, and Windows Mail—could be."

DISABLING IPV6 IN WINDOWS

What breaks if IPv6 is disabled on Windows Vista and Later?

- Hyper-V Cluster - It is not possible to add a new node to an existing cluster
- TMG Server - RRAS breaks
- Exchange - Mail flow & Installation problems
- SBS Server - Exchange services fail to start & network shows offline
- DirectAccess - Does not work
- HomeGroup - Does not work
- Applications using Windows Peer-to-Peer Networking will not work