IPv6 Security: Myths and Reality

Eric Vyncke, Distinguished Engineer, evyncke@cisco.com

IPv6 Myths: Better, Faster, More Secure

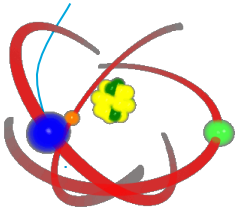
Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

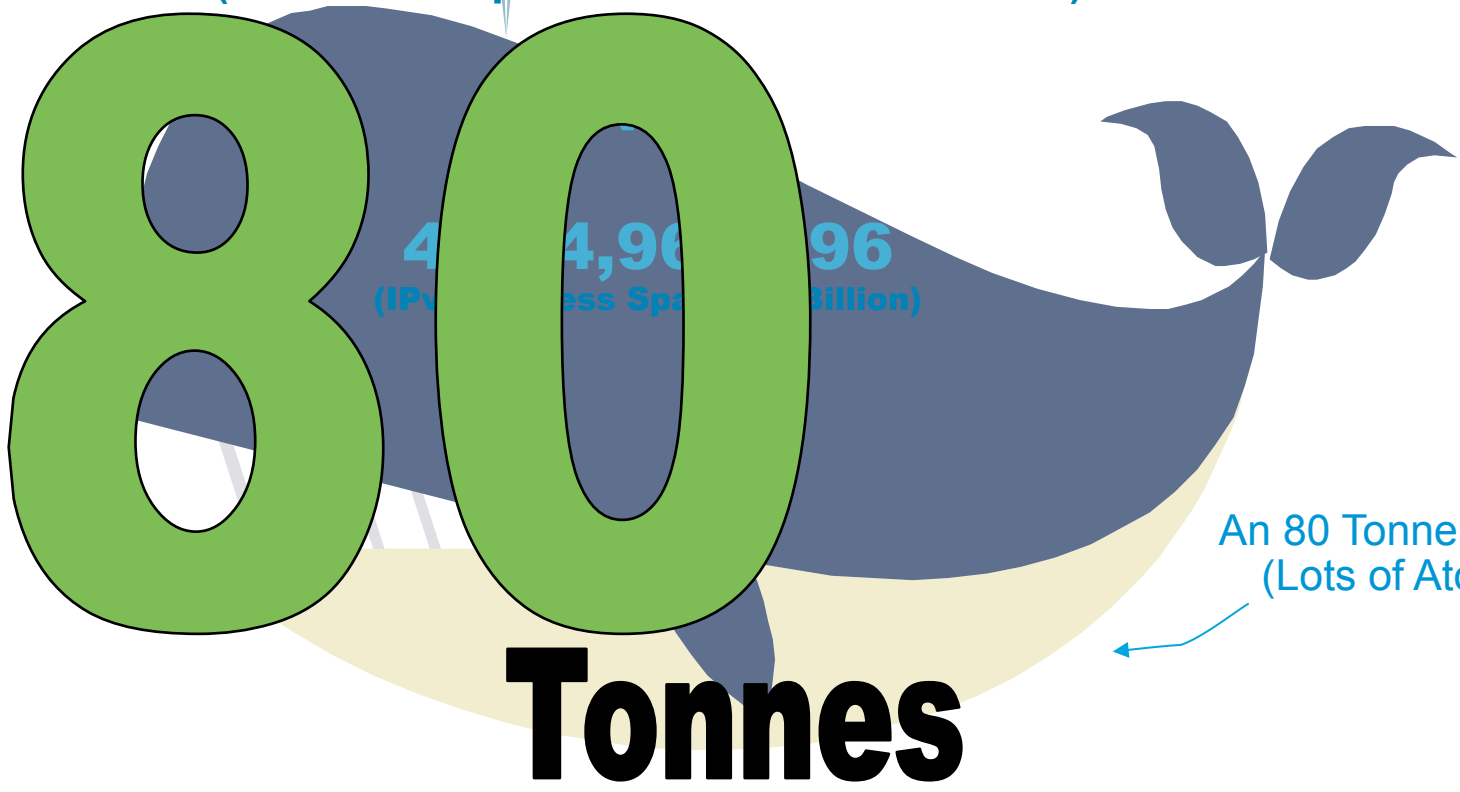
So How Big Is The IPv6 Address Space?

340,282,366,920,938,463,374,607,432,768,211,456

(IPv6 Address Space - 340 Trillion Trillion Trillion)



An Atom



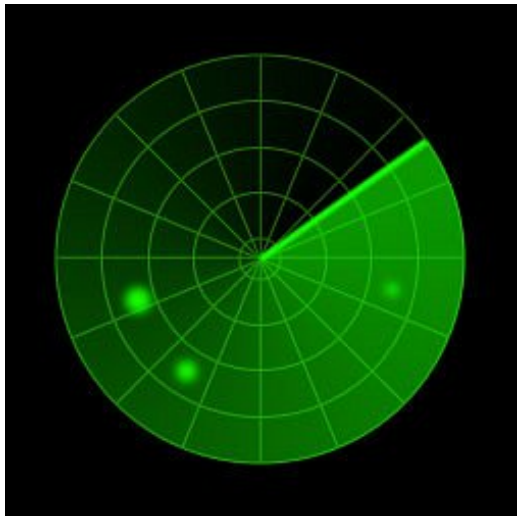
An 80 Tonne Whale
(Lots of Atoms)

- Let's assume that an atom represents 4 Billion Addresses
- You would need 80,000 Kgs of Atoms to represent IPv6!!!!

Reconnaissance in IPv6
Subnet Size Difference

- Default subnets in IPv6 have 2^{64} addresses
  - 10 Mpps = more than 50 000 years
- NMAP doesn't even support ping sweeps on IPv6 networks, it only works for port scans

Reconnaissance in IPv6
Scanning Methods Are Likely to Change



- Public servers will still need to be DNS reachable
  - ⇒More information collected by Google...
- Increased deployment/reliance on dynamic DNS
  - ⇒More information will be in DNS
- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses (:: 10,::20,::F00D, ::C5C0, :ABBA:BABE or simply IPv4 last octet for dual stack)
- By compromising hosts in a network, an attacker can learn new addresses to scan
- Transition techniques derive IPv6 address from IPv4 address
  - ⇒ can scan again

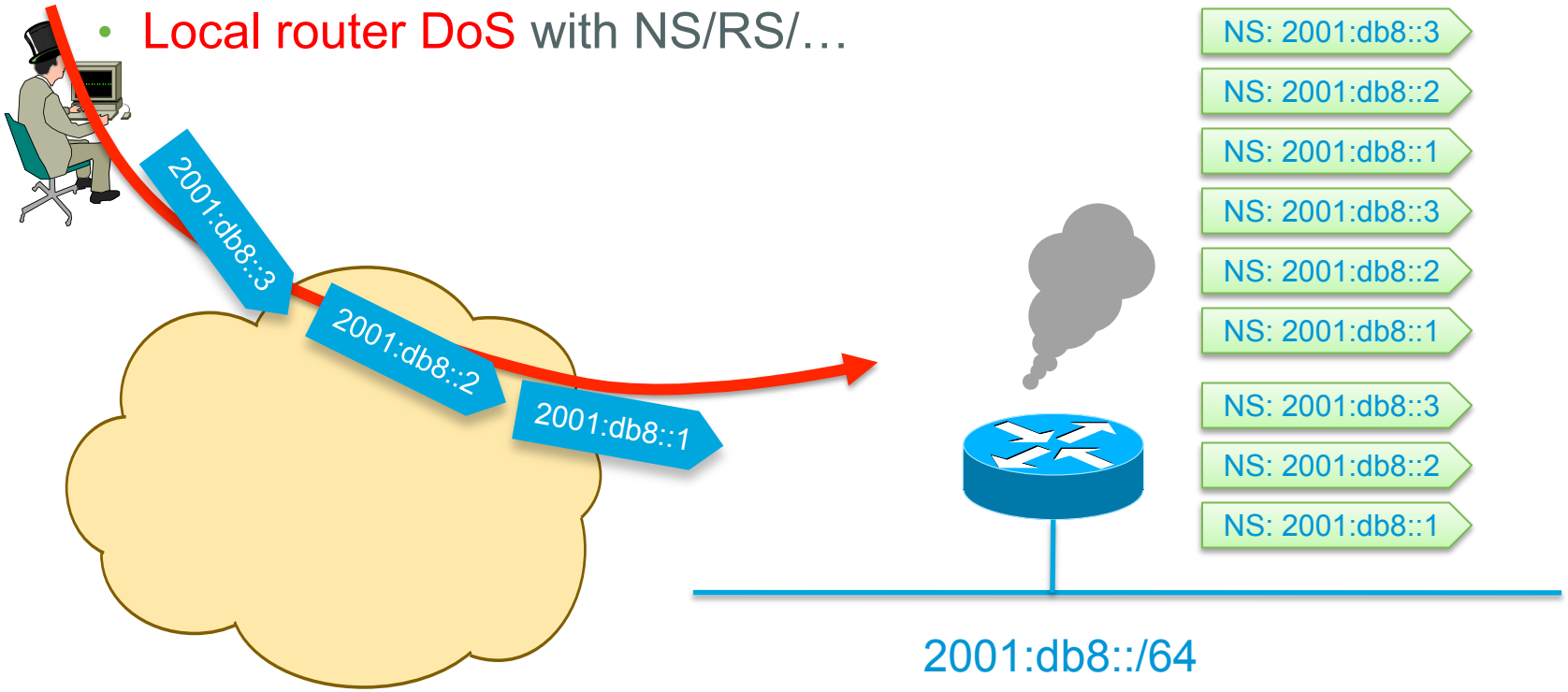
IPv6 huge addressing space was never design to prevent scanning, only to allow Internet growth ;-)

Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion

- Remote router CPU/memory DoS attack if aggressive scanning

  Router will do Neighbor Discovery... And waste CPU and memory

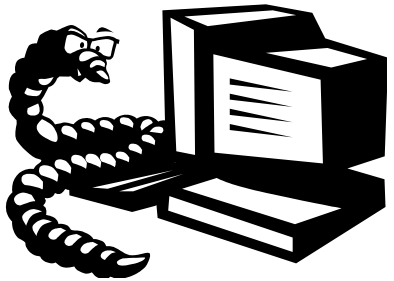
- Local router DoS with NS/RS/…



Mitigating Remote Neighbor Cache Exhaustion

- Built-in rate limiter with options to tune it
  - Since 15.1(3)T: **`ipv6 nd cache interface-limit`**
  - Or IOS-XE 2.6: **`ipv6 nd resolution data limit`**
  - **Destination-guard** is part of First Hop Security phase 3
  - Priority given to refresh existing entries vs. discovering new ones
- Using a /64 on **point-to-point links** => a lot of addresses to scan!
  - Using /127 could help (RFC 6164)
- **Internet edge/presence**: a target of choice
  - Ingress ACL permitting traffic to specific statically configured (virtual) IPv6 addresses only
- Using infrastructure ACL prevents this scanning
  - iACL: edge ACL denying packets addressed to your routers
  - Easy with IPv6 because new addressing scheme ☺

Viruses and Worms in IPv6



- Viruses and email, IM worms: IPv6 brings no change
- Other worms:

  IPv4: reliance on network scanning

  IPv6: not so easy (see reconnaissance) => will use alternative techniques

- Worm developers will adapt to IPv6
- IPv4 best practices around worm detection and mitigation remain valid

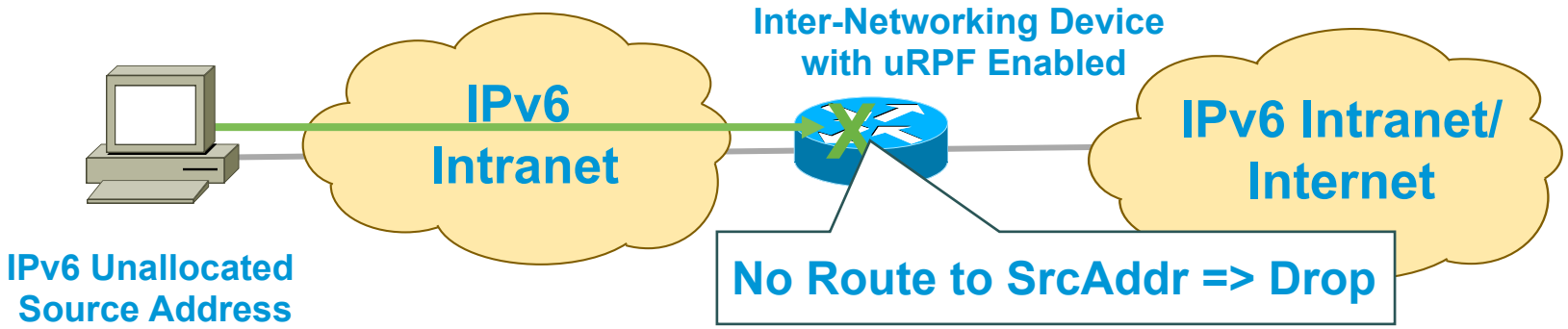
The IPsec Myth:
IPsec End-to-End will Save the World

- In 1997, IPv6 mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 "*IPsec SHOULD be supported by all IPv6 nodes*"
- Some organizations believe that IPsec should be used to secure all flows...
  - Interesting **scalability** issue
  - Need to **trust endpoints and end-users** because the network cannot secure the traffic: no IPS, no ACL, no firewall
  - Network **telemetry is blinded**: IPfix, NetFlow of little use
  - Network **services hindered**: what about QoS?

Recommendation: do not use IPsec end to end within an administrative domain.
Suggestion: Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4

IPv6 Bogon and Anti-Spoofing Filtering

- Same as in IPv4
- Bogon filtering (data plane & BGP route map): http://www.cymru.com/Bogons/ipv6.txt
- Anti-spoofing: uRPF



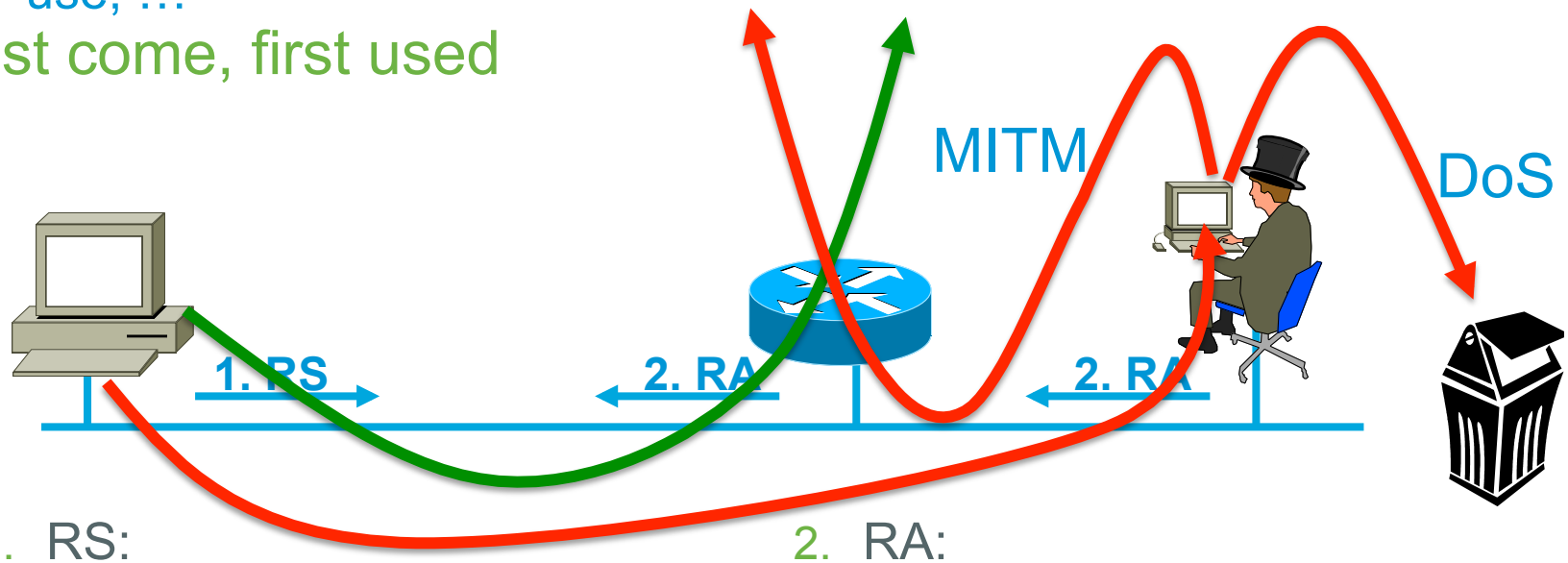
Rogue Router Advertisement

RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)

Router Advertisements contain:

- -Prefix to be used by hosts
- -Data-link layer address of the router
- -Miscellaneous options: MTU, DHCPv6 use, …

Last come, first used



1. RS:
   Data = Query: please send RA
2. RA:
   Data= options, **prefix**, lifetime, A+M+O flags

Effect of Rogue Router Advertisements

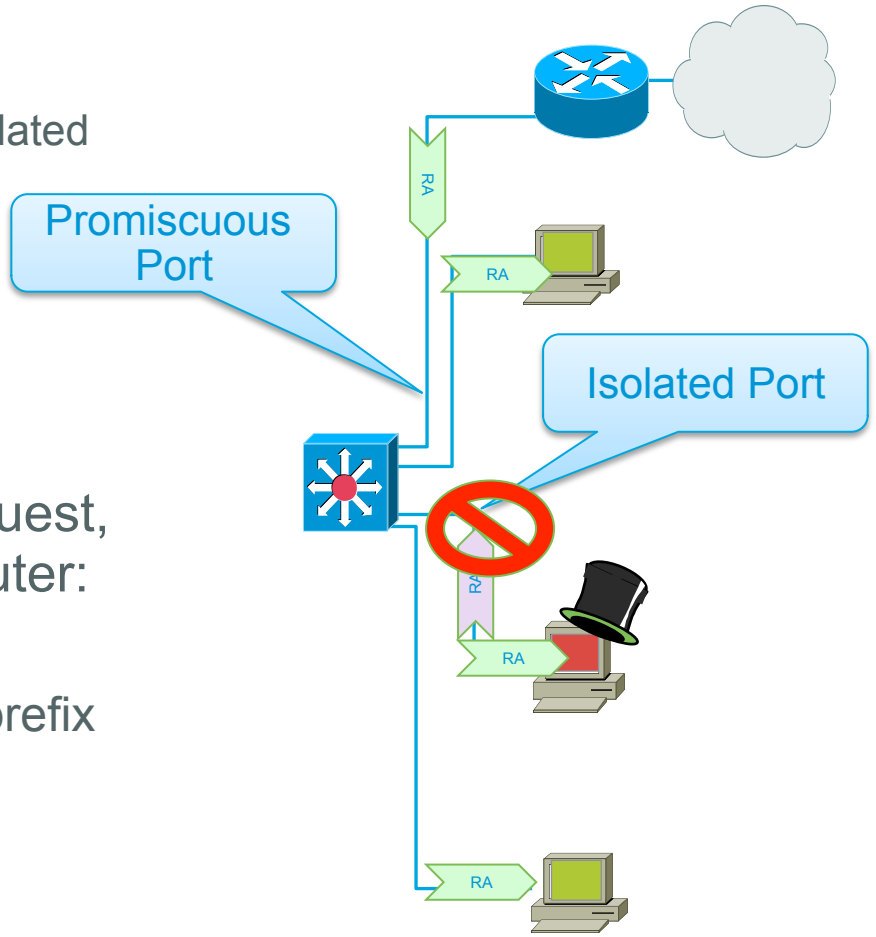
- Devastating:
  - Denial of service: all traffic sent to a black hole
  - Man in the Middle attack: attacker can intercept, listen, modify unprotected data
- Also affects legacy IPv4-only network with IPv6-enabled hosts
- Most of the time from non-malicious users
- Requires layer-2 adjacency (some relief…)
- It was the major blocking factor for enterprise IPv6 deployment pretty much like IPv4 ARP spoofing/rogue DHCPv4

ARP Spoofing is now NDP Spoofing: Mitigation

- **GOOD NEWS**: dynamic ARP inspection for IPv6 is available
  - First phase (Port ACL & RA Guard) available in Cisco IOS since Summer 2010
  - Second phase (NDP & DHCP snooping) available in Cisco IOS since Summer 2011
  - http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- **(kind of) GOOD NEWS**: Secure Neighbor Discovery
  - SeND = NDP + crypto
  - IOS 12.4(24)T
  - But not in Windows Vista, 2008 and 7, Mac OS/X, iOS, Android
  - Crypto means slower...
- Other **GOOD NEWS**:
  - Private VLAN works with IPv6
  - Port security works with IPv6
  - IEEE 801.X works with IPv6 (except downloadable ACL)

Mitigating Rogue RA: Host Isolation

- Prevent Node-Node Layer-2 communication by using:
  - Private VLANs (PVLAN) where nodes (isolated port) can only contact the official router (promiscuous port)
  - WLAN in ‘AP Isolation Mode’
  - 1 VLAN per host (SP access network with Broadband Network Gateway)
- Link-local multicast (RA, DHCP request, etc) sent only to the local official router: no harm done by rogue RA
  - Side effect: it also disables DAD... If prefix is advertised as on-link



Mitigating Rogue RA: RFC 6101

- **Port ACL** blocks all ICMPv6 RA from hosts

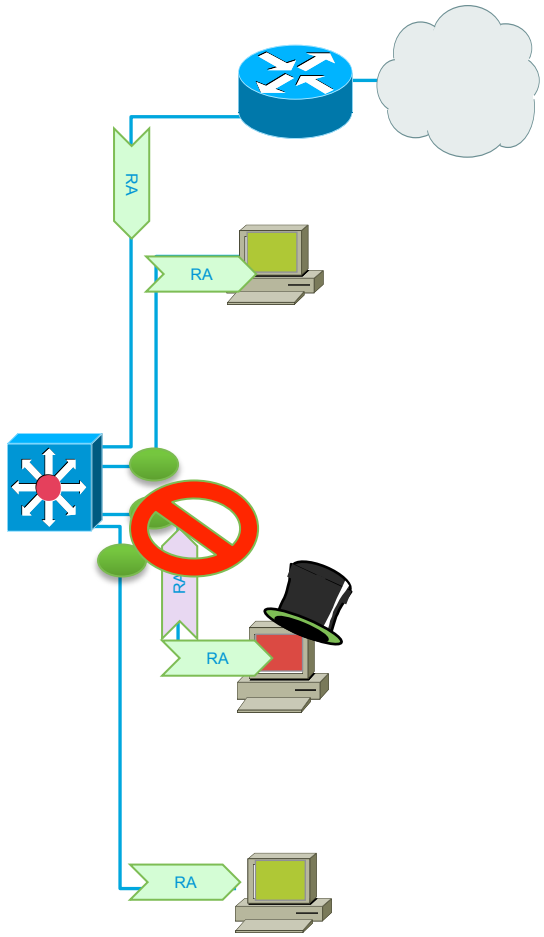
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **RA-guard lite** (12.2(33)SXI4 & 12.2(54)SG): also dropping all RA received on this port

```
interface FastEthernet0/2
  ipv6 nd raguard
  access-group mode prefer port
```

- **RA-guard** (12.2(50)SY, 15.0(2)SE)

```
ipv6 nd raguard policy HOST device-role host
ipv6 nd raguard policy ROUTER device-role router
ipv6 nd raguard attach-policy HOST vlan 100
interface FastEthernet0/0
  ipv6 nd raguard attach-policy ROUTER
```



ICMPv4 vs. ICMPv6

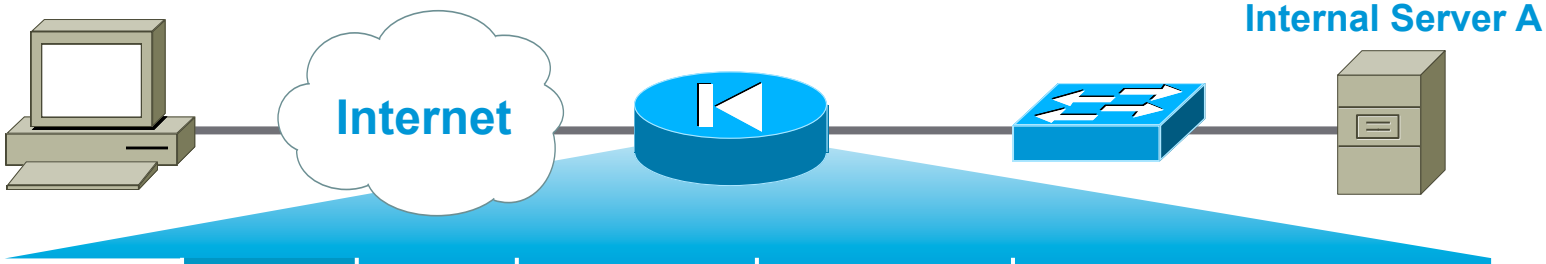
- Significant changes
- More relied upon

ICMP Message Type	ICMPv4	ICMPv6
Connectivity Checks	X	X
Informational/Error Messaging	X	X
Fragmentation Needed Notification	X	X
Address Assignment		X
Address Resolution		X
Router Discovery		X
Multicast Group Management		X
Mobile IPv6 Support		X

- => ICMP policy on firewalls needs to change

Generic ICMPv4
Border Firewall Policy

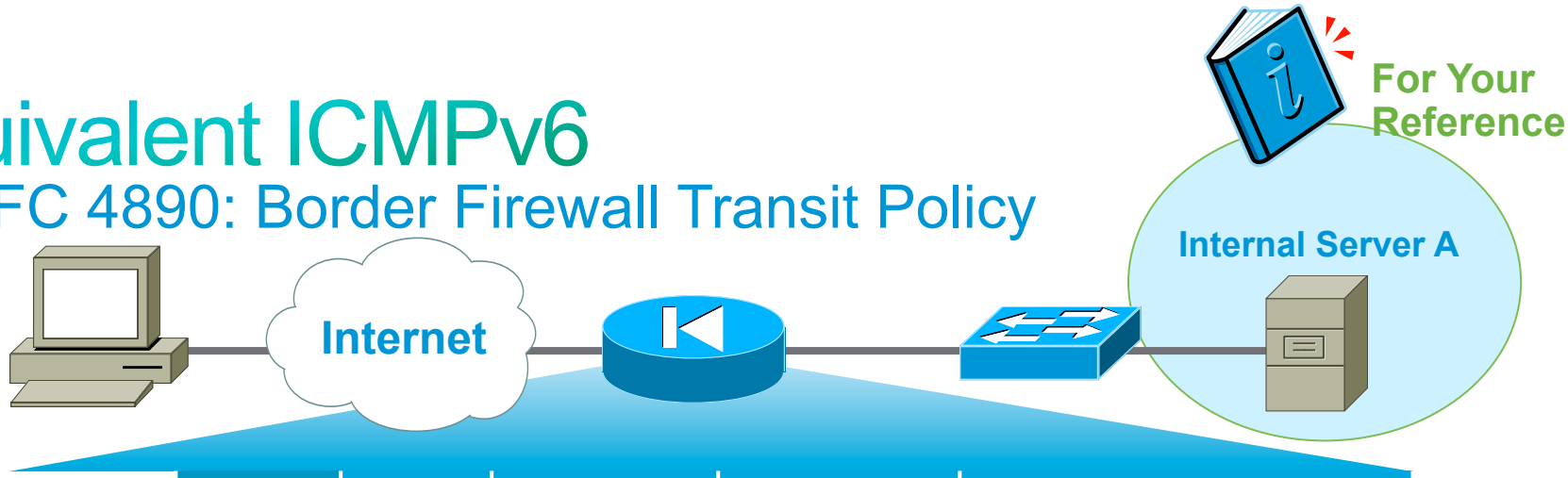
For Your Reference



Action	Src	Dst	ICMPv4 Type	ICMPv4 Code	Name
Permit	Any	A	0	0	Echo Reply
Permit	Any	A	8	0	Echo Request
Permit	Any	A	3	0	Dst. Unreachable—Net Unreachable
Permit	Any	A	3	4	Dst. Unreachable—Frag. Needed
Permit	Any	A	11	0	Time Exceeded—TTL Exceeded

Equivalent ICMPv6

RFC 4890: Border Firewall Transit Policy



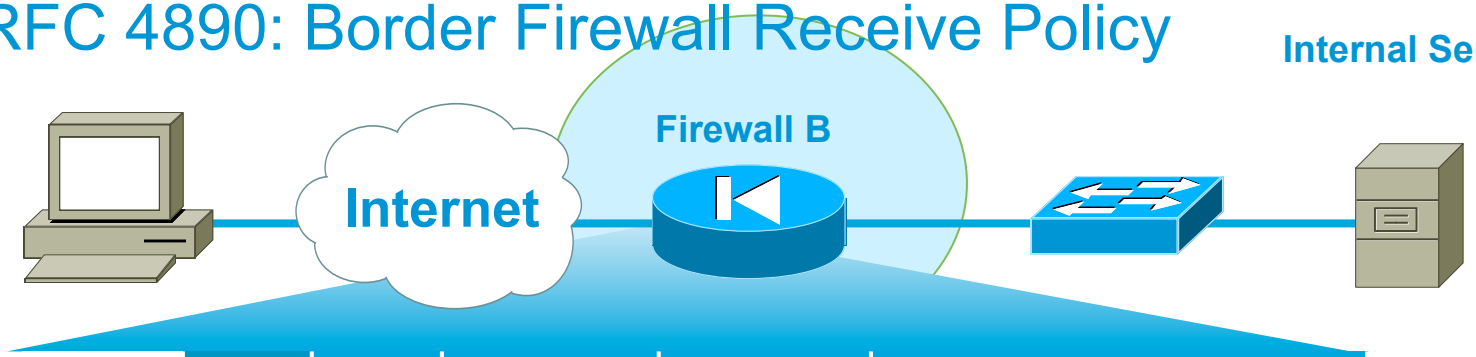
Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	No Route to Dst.
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—TTL Exceeded
Permit	Any	A	4	0	Parameter Problem

Needed for Teredo traffic

Potential Additional ICMPv6

RFC 4890: Border Firewall Receive Policy

For Your Reference



Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	135/136	0	Neighbor Solicitation and Advertisement
Deny	Any	Any			

For locally generated traffic

IPv6 Attacks with Strong IPv4 Similarities

- Application layer attacks

  The majority of vulnerabilities on the Internet today are at the application layer, something that IPSec will do nothing to prevent

- Rogue devices

  Rogue devices will be as easy to insert into an IPv6 network as in IPv4

- Man-in-the-Middle Attacks (MITM)

  Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

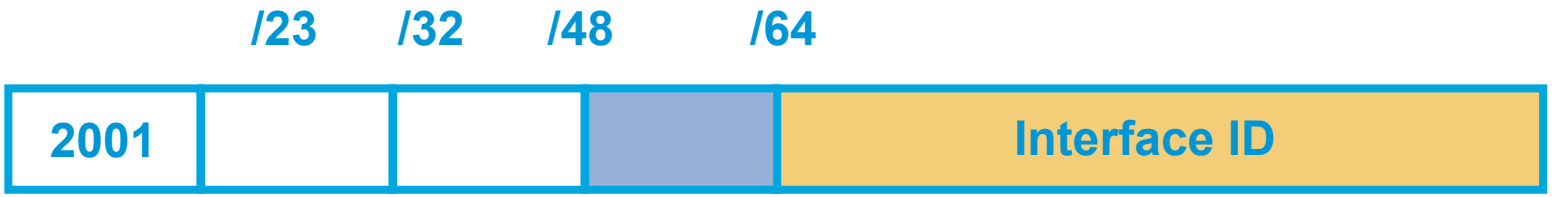
- Flooding

  Flooding attacks are identical between IPv4 and IPv6

- Sniffing

  IPv6 is no more or less likely to fall victim to a sniffing attack than IPv4

IPv6 Privacy Extensions (RFC 4941) A.K.A. Temporary Addresses



- Temporary addresses for IPv6 host client application, e.g. web browser
  - Inhibit device/user tracking
  - Random 64 bit interface ID, then run Duplicate Address Detection before using it
  - Rate of change based on local policy
- Enabled by default in Windows, Android, iOS 4.3, Mac OS/X 10.7

Recommendation: Use Privacy Extensions for External Communication but not for Internal Networks (Troubleshooting and Attack Trace Back)

IETF Work in progress: unpredictable but stable addresses

Is there NAT for IPv6? “I need it for security”

- Network Prefix Translation, RFC 6296,
  - 1:1 stateless prefix translation allowing all inbound/outbound packets.
  - Main use case: multi-homing
- Else, IETF has not specified any N:1 stateful translation (aka overload NAT or NAPT) for IPv6
  - IETF has not specified N:1 or 1:1 NAT for IPv4 anyway, this is a vendor thing
- Do not mix stateful firewall and NAPT even if they are often co-located

- Nowadays, NAPT (for IPv4) does not help security
  - Host OS are way more resilient than in 2000
  - Hosts are mobile and cannot always be behind your ‘controlled NAPT’
  - Malware are not injected from ‘outside’ but are fetched from the ‘inside’ by visiting weird sites or installing any trojanized application
  - Nearly 80% of the Torpig-infected hosts were behind a NAPT...

> *"By looking at the IP addresses in the Torpig headers we are able to determine that 144,236 (78.9%) of the infected machines were behind a NAT, VPN, proxy, or firewall. We identified these hosts by using the non-publicly routable IP addresses listed in RFC 1918: 10/8, 192.168/16, and 172.16-172.31/16"*

Stone-Gross et al., "*Your Botnet is My Botnet: Analysis of a Botnet Takeover*", 2009

http://www.cs.ucsb.edu/~rgilbert/pubs/torpig_ccs09.pdf

PCI DSS 2.0 Compliance and IPv6

- Payment Card Industry Data Security Standard *(latest revision October 2010)*:

  Requirement 1.3.8 *Do not disclose private IP addresses and routing information to unauthorized parties.*

  Note: Methods to obscure IP addressing may include, but are not limited to: Network Address Translation (NAT)

- ➔ how to comply with PCI DSS

  Application proxies or SOCKS

  Strict data plane filtering with ACL

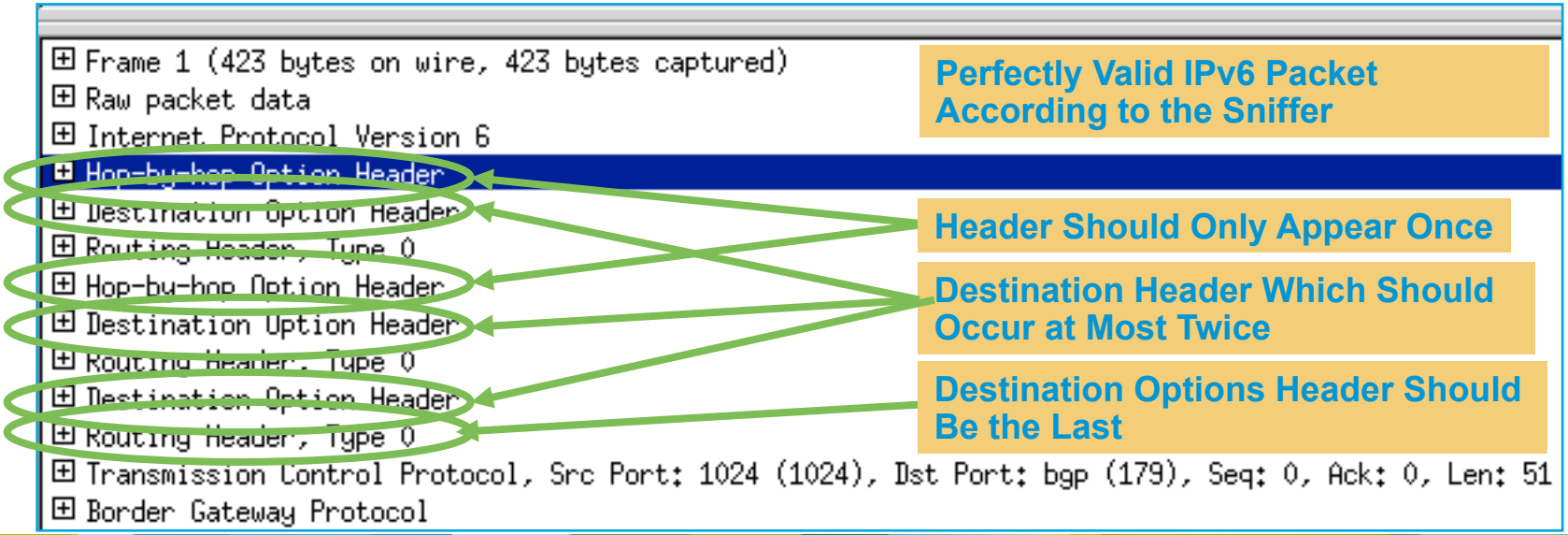
  Strict routing plane filtering with BGP route-maps

- Cisco IPv6 design for PCI with IPv6

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Compliance/Compliance_DG/PCI_20_DG.pdf

IPv6 Header Manipulation

- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations
  - More boundary conditions to exploit
  - Can I overrun buffers with a lot of extension headers?
- Mitigation: use firewall or IPS to drop packets which violate extension header specification



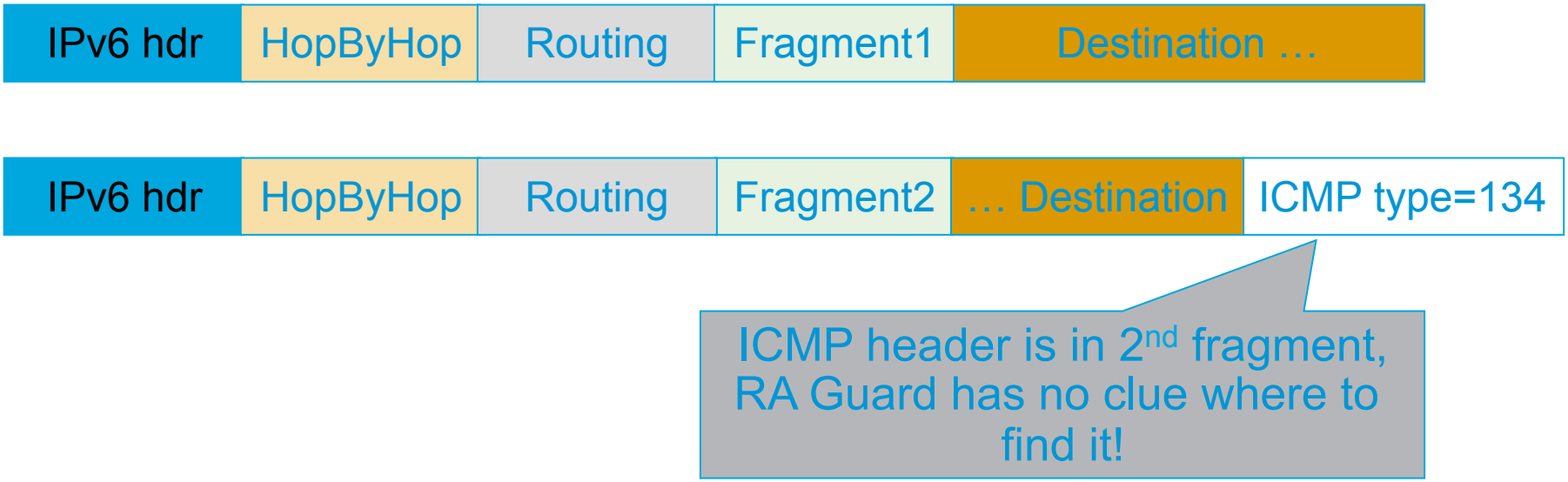
See also: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **MATCH**
  - Or unknown extension header/layer 4 header found... => **NO MATCH**

Parsing the Extension Header Chain Fragments and Stateless Filters (RA Guard)

- RFC 3128 is not applicable to IPv6, extension header can be fragmented
- ICMP header could be in 2nd fragment after a fragmented extension header
- RA Guard works like a stateless ACL filtering ICMP type 134
- THC `fake_router6 -FD` implements this attack which bypasses RA Guard
- Partial work-around: block all fragments sent to ff02::1
- If supported, deny undetermined-transport blocks this attack (work item at IETF)

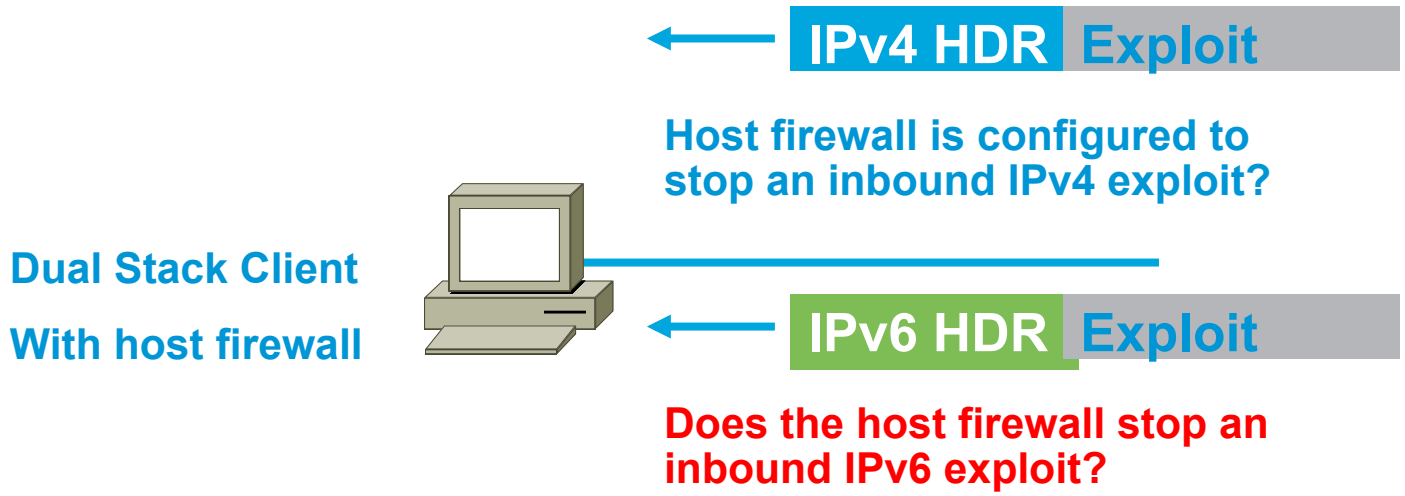


IPv4 to IPv6 Transition Challenges

- 16+ methods, possibly in combination
- Dual stack
  - Consider security for both protocols
  - Cross v4/v6 abuse
  - Resiliency (shared resources)
- Tunnels
  - Bypass firewalls (protocol 41 or UDP)
  - Can cause asymmetric traffic (hence breaking stateful firewalls)

Dual Stack Host Considerations

- Host security on a dual-stack device
  - Applications can be subject to attack on both IPv6 and IPv4
  - **Fate sharing**: as secure as the least secure stack...
- Host security controls should block and inspect traffic from both IP versions
  - Host intrusion prevention, personal firewalls, VPN clients, etc.



Dual Stack with Enabled IPv6 by Default

- Your host:
  - IPv4 is protected by your favorite personal firewall...
  - IPv6 is enabled by default (Vista, Linux, Mac OS/X, ...)
- Your network:
  - Does not run IPv6
- Your assumption:
  - I'm safe
- Reality
  - You are **not** safe
  - Attacker sends Router Advertisements
  - Your host configures silently to IPv6
  - You are now under IPv6 attack
- => Probably time to think about IPv6 in your network

Vulnerability Scanning in a Dual-Stack World

- Finding all hosts:
  - Address enumeration does not work for IPv6
  - Need to rely on DNS or NDP caches or NetFlow
- Vulnerability scanning
  - IPv4 global address, IPv6 global address(es) (if any), IPv6 link-local address
  - Some services are single stack only (currently mostly IPv4 but who knows...)
  - Personal firewall rules could be different between IPv4/IPv6
- **IPv6 vulnerability scanning MUST be done for IPv4 & IPv6 even in an IPv4-only network**
  - IPv6 link-local addresses are active by default

IPv6 can be secured as IPv4
FYI Summary of Cisco IPv6 Security Products

- ASA Firewall
  - Since version 7.0 (released 2005)
  - Flexibility: Dual stack, IPv6 only, IPv4 only
  - SSL VPN for IPv6 over IPv4 (ASA 8.0) over IPv6 (ASA 9.0)
  - Stateful-Failover (ASA 8.2.2)
  - Extension header filtering and inspection (ASA 8.4.2)
  - Dual-stack ACL & object grouping (ASA 9.0)
- ASA-SM
  - Leverage ASA code base, same features ;-) 16 Gbps of IPv6 throughput
- IOS Firewall
  - IOS 12.3(7)T (released 2005)
  - Zone-based firewall on IOS-XE 3.6 (2012)
- IPS
  - Since 6.2 (released 2008)
- Email Security Appliance (ESA) under beta testing since 2010, IPv6 support since 7.6.1 (May 2012)
- Web Security Appliance (WSA) with explicit proxy then transparent mode, work in progress (end of 2013 or early 2014)
- Cisco Cloud Web Security (ScanSafe) expected to be available in 2013 or early 2014

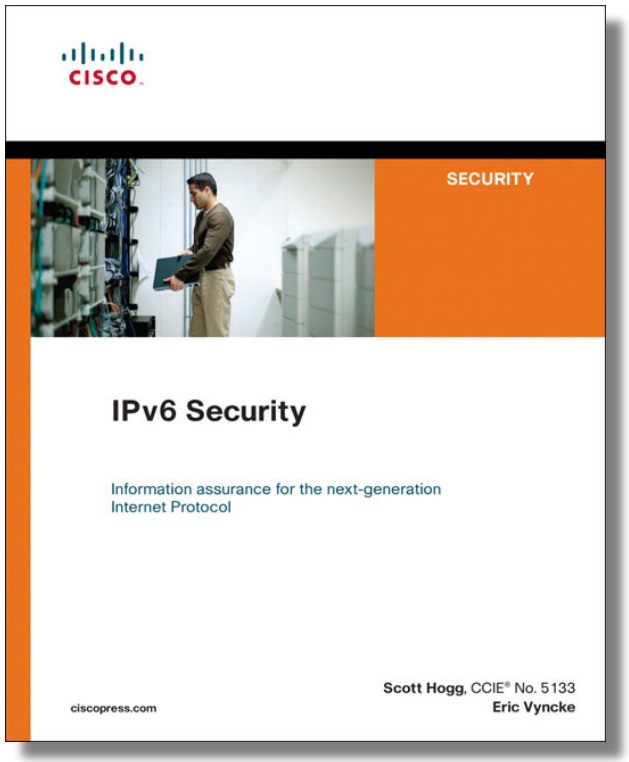
Summary

Key Take Away

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and more features coming
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
  - Fragmentation: undetermined-transport is your friend
- Lack of operation experience may hinder security for a while: **training is required**
- Security enforcement is possible, IETF and the industry have done a good job
  - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when suitable

Questions and Answers?

Recommended Reading



Source: Cisco Press