IPv6 Security

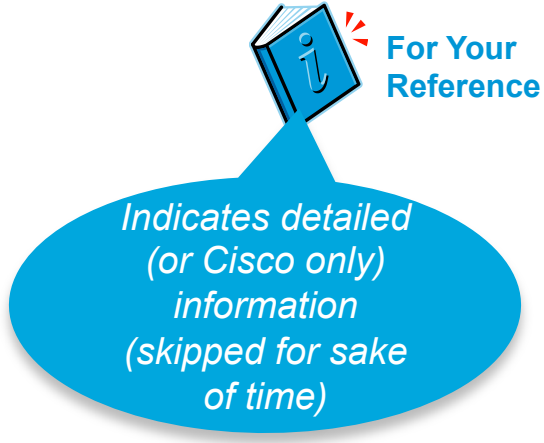
Eric Vyncke, Distinguished Engineer
evyncke@cisco.com
@evyncke

October 2014

Agenda

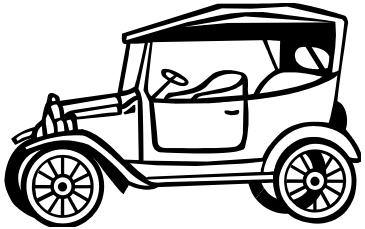
- Debunking IPv6 Myths
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6

  Extension headers, IPsec everywhere, tunneling techniques
- Enforcing a Security Policy in IPv6
- Summary



IPv6 Security Myths…

IPv6 Myths: Better, Faster, More Secure



Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

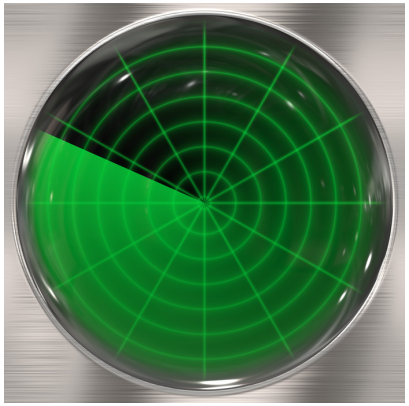
Source: Microsoft clip-art gallery

The Absence of Reconnaissance Myth

- Default subnets in IPv6 have 2^{64} addresses
  - 10 Mpps = more than 50 000 years

Source: Microsoft clip-art gallery

Reconnaissance in IPv6 Scanning Methods Will Change



Source: Microsoft clip-art gallery

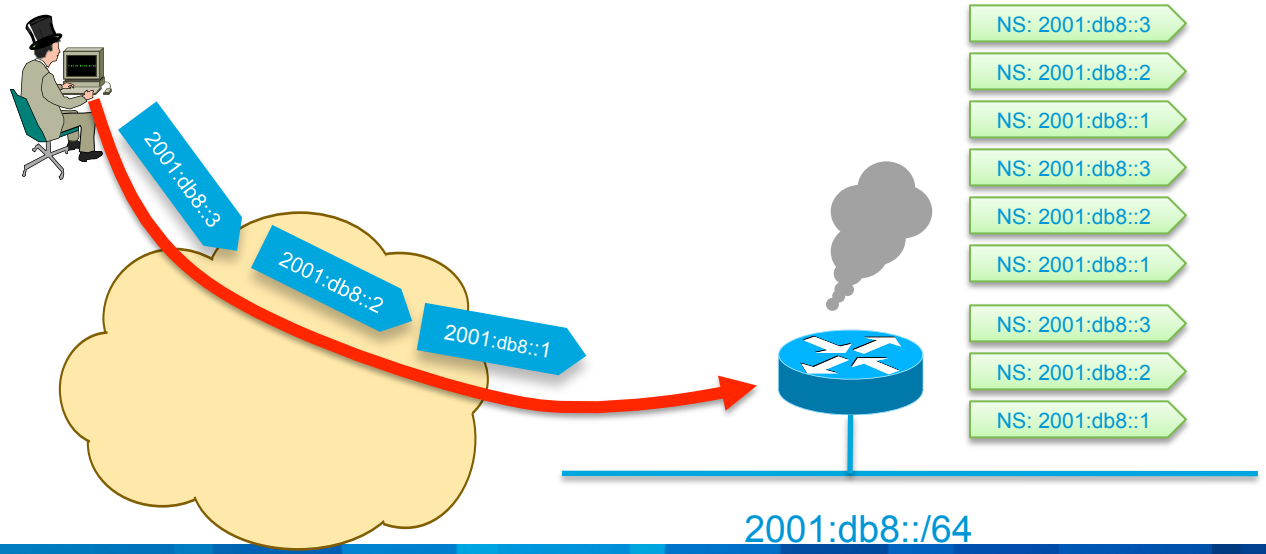
- If using EUI-64 addresses, just scan 2^{48}
  - Or even 2^{24} if vendor OUI is known...
- Public servers will still need to be DNS reachable
  - More information collected by Google...
- Increased deployment/reliance on dynamic DNS
  - More information will be in DNS
- Using peer-to-peer clients gives IPv6 addresses of peers
- Administrators may adopt easy-to-remember addresses
  - ::1,::80,::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

Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion (RFC 6583)

- Potential router CPU/memory attacks 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

  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 ☺

http://www.insinuator.net/2013/03/ipv6-neighbor-cache-exhaustion-attacks-risk-assessment-mitigation-strategies-part-1

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

- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 6434 "*IPsec SHOULD be supported by all IPv6 nodes*"
- Some organizations still believe that IPsec should be used to secure all flows...

  Need to **trust endpoints** and end-users because the network cannot secure the traffic: no IPS, no ACL, no firewall

  Network **telemetry** is blinded: NetFlow of little use

  Network **services** hindered: what about QoS or AVC ?

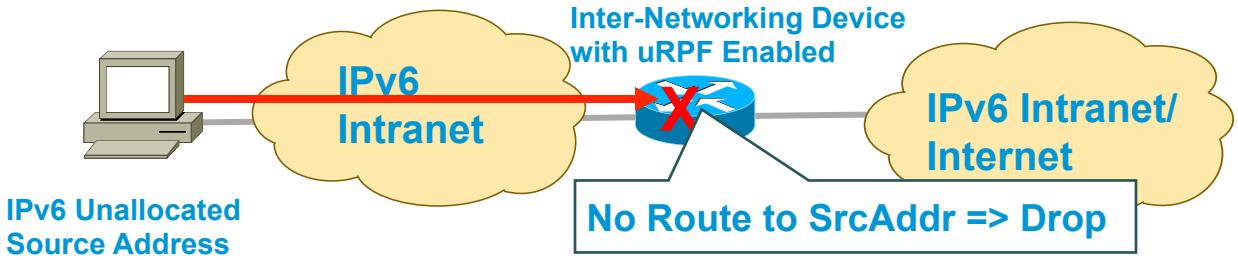
Recommendation: do not use IPsec end to end within an administrative domain.

Suggestion: Reserve IPsec for residential or hostile environment or high profile targets EXACTLY as for IPv4

Shared Issues

IPv6 Bogon and Anti-Spoofing Filtering

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

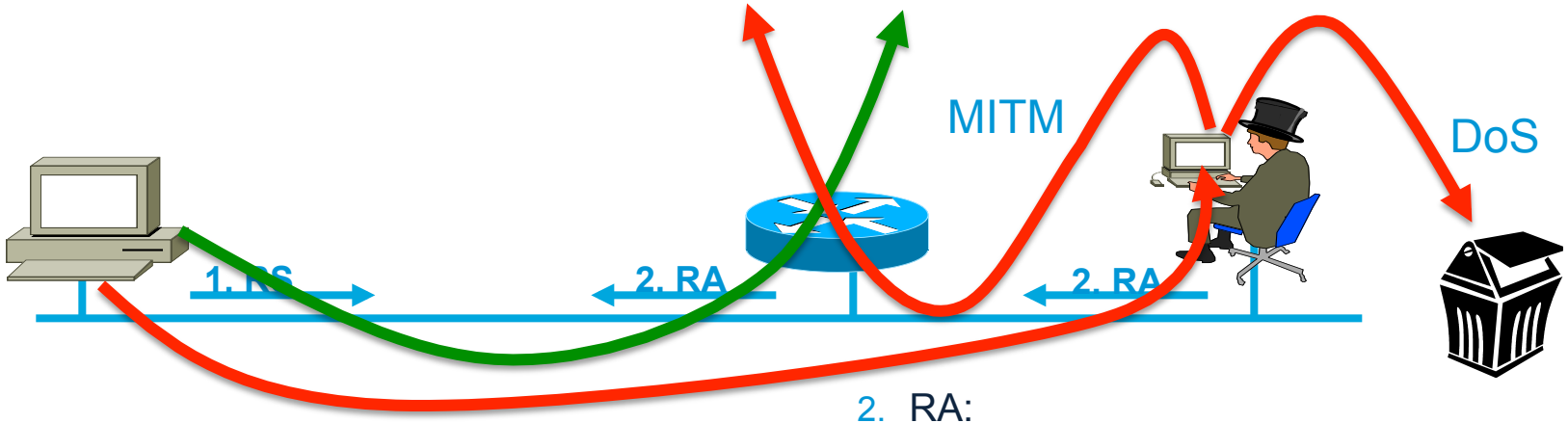


Neighbor Discovery Issue#1 StateLess Address AutoConfiguration SLAAC Rogue Router Advertisement

Router Advertisements (RA) contains:

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

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



1. RS:

   Data = Query: please send RA

2. RA:

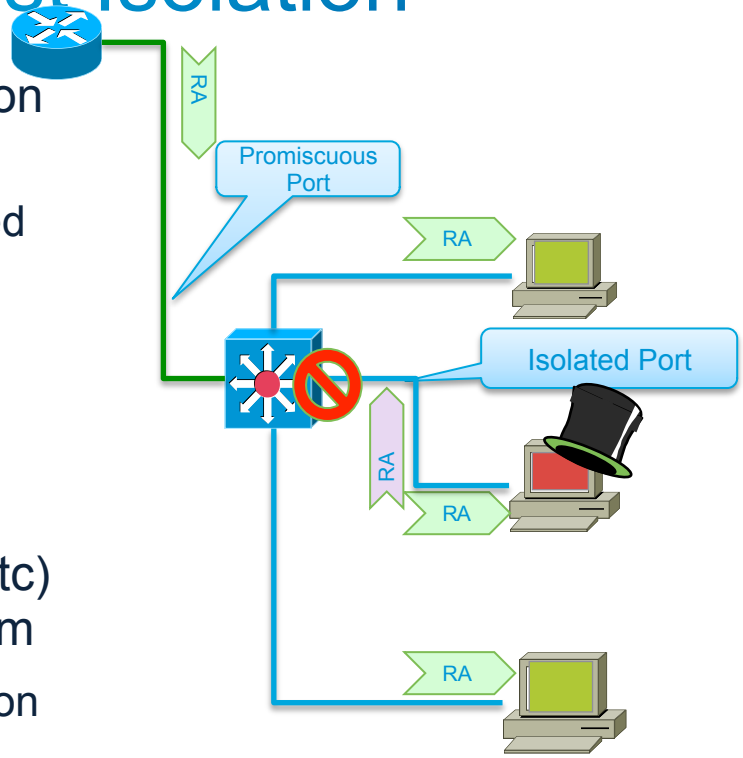
   Data= options, prefix, lifetime, A+M+O flags

ARP Spoofing is now NDP Spoofing: Mitigation

- **GOOD NEWS**: First-Hop-Security for IPv6 is available
  - First phase (Port ACL & RA Guard) available since Summer 2010
  - Second phase (NDP & DHCP snooping) available since Summer 2011
  - Third phase (Source Guard, Destination Guard) available since Summer 2013
  - 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 7, 2008, 2012 and 8, Mac OS/X, iOS, Android
- 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
  - Side effect: breaks Duplicate Address Detection (DAD)



First Hop Security: RAguard since 2010 (RFC 6105)

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

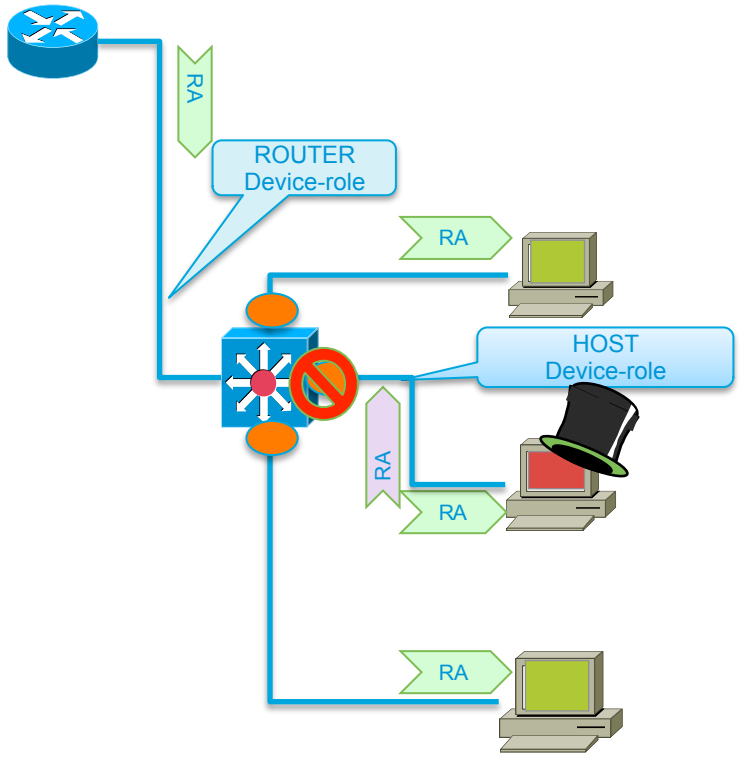
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **RAguard 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
```

- **RAguard** (12.2(50)SY, 15.0(2)SE)

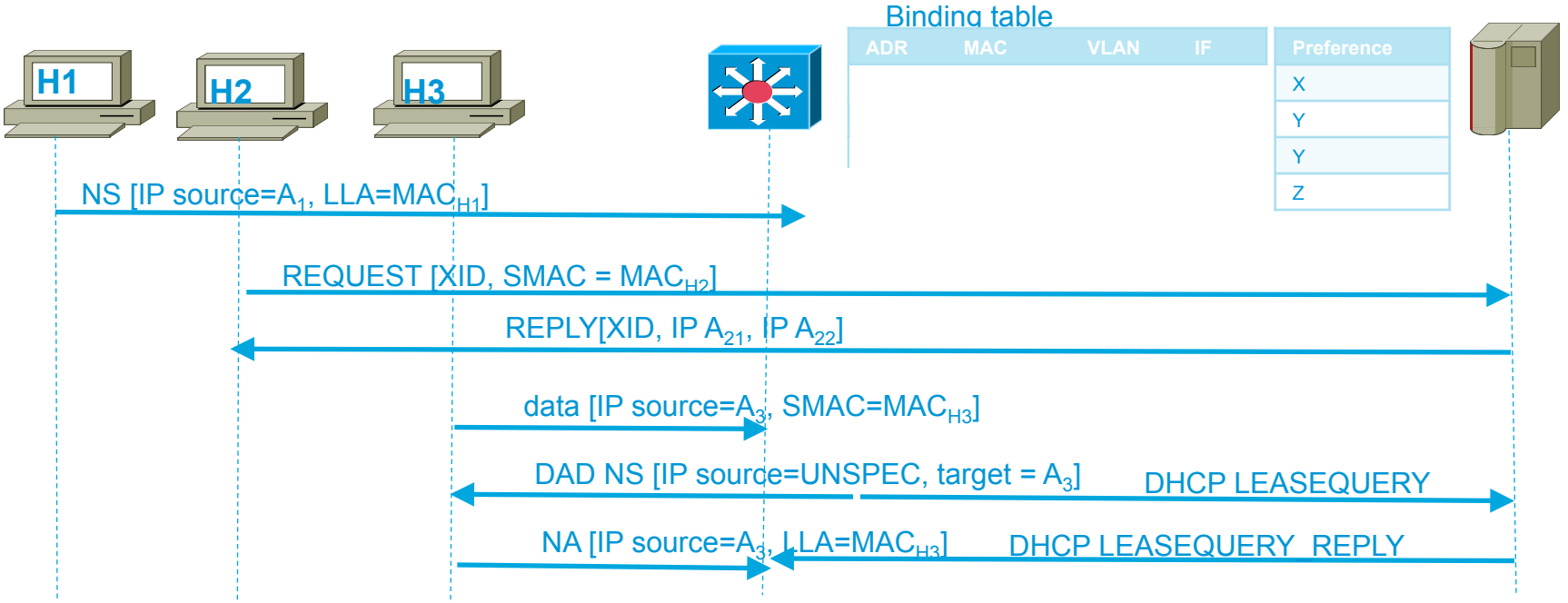
```
ipv6 nd raguard policy HOST device-role host
ipv6 nd raguard policy ROUTER device-role router
ipv6 nd raguard attach-policy HOST vlan 100
interface FastEthernet0/0
  ipv6 nd raguard attach-policy ROUTER
```



Binding Integrity Guard: GLEAN (RFC 6620)

Address ownership vulnerabilities mitigation on First Hop

For Your Reference



Then use those bindings to drop invalid NDP packets

IPv6 and the LAN Access

IPv6 FHS	C6K	C4500-X C4500 C4900	C3750-X C3560-X C29602 Compact	WLC
RA Guard	12.2(50)SY and 15.0(1)SY	12.2(54)SG	15.0(2)SE	7.2
DHCP Guard	15.2(1)SY	XE 3.4.xSG 15.1(2)SG	15.0(2)SE	7.2
Binding Integrity Guard	15.2(1)SY	XE 3.4.xSG 15.1(2)SG	15.0(2)SE	7.2
Source Guard	15.2(1)SY	15.2(1)E	15.0(2)SE	7.2
Destination Guard	15.2(1)SY	XE 3.4.xSG 15.1(2)SG	15.0(2)SE	7.2

ICMPv4 vs. ICMPv6

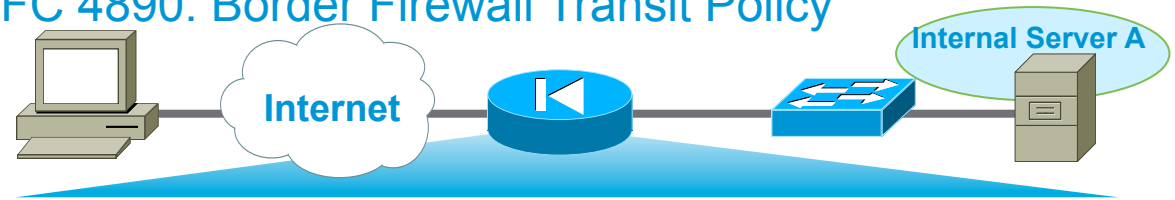
- Significant changes
- More relied upon

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

Equivalent ICMPv6

RFC 4890: Border Firewall Transit Policy

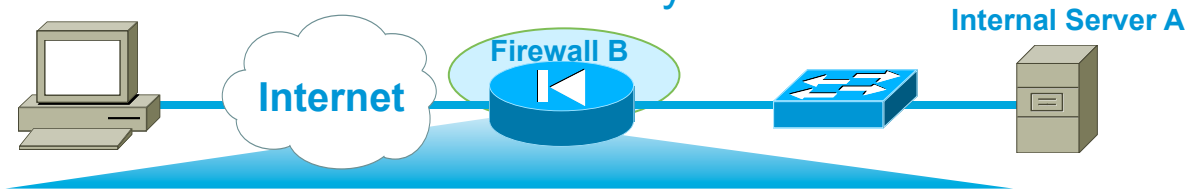


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	Unreachable
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—HL Exceeded
Permit	Any	A	4	0	Parameter Problem

Needed for Teredo traffic

Potential Additional ICMPv6

RFC 4890: Border Firewall Receive Policy



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 by the device

IPv6 Attacks with Strong IPv4 Similarities

- Sniffing

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

- 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)

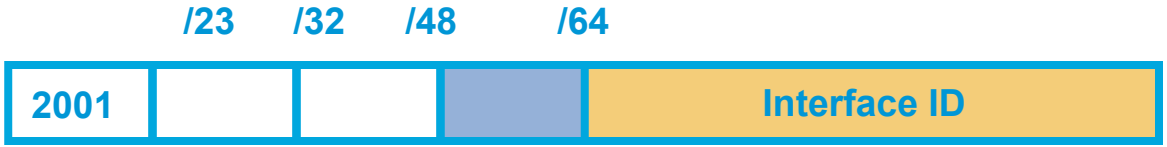
  Without strong mutual authentication, any attacks utilizing MITM will have the same likelihood in IPv6 as in IPv4

- Flooding

  Flooding attacks are identical between IPv4 and IPv6

Specific IPv6 Issues

IPv6 Privacy Extensions (RFC 4941) AKA 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)

For Your Reference

Disabling Privacy Extension

- Disabling stateless auto-configuration and force DHCPv6

  Send Router Advertisements with

  all prefixes with A-bit set to 0 (disable SLAAC)

  M-bit set to 1 to force stateful DHCPv6

  Use DHCP to a specific pool + ingress ACL allowing only this pool

```
interface fastEthernet 0/0
  ipv6 nd prefix default no-autoconfig
  ipv6 dhcp server . . . (or relay)
  ipv6 nd managed-config-flag
```

Parsing the Extension Header Chain

- Finding the layer 4 information is not trivial in IPv6

  Skip all known extension header

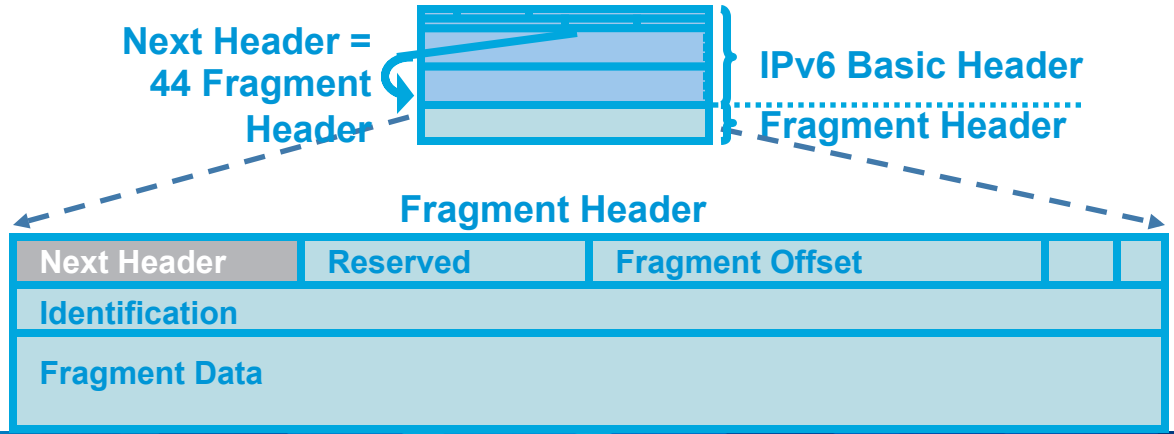
  Until either known layer 4 header found => **MATCH**

  Or unknown extension header/layer 4 header found... => **NO MATCH**

Fragment Header: IPv6

- In IPv6 fragmentation is done only by the end system

  Tunnel end-points are end systems => Fragmentation / re-assembly can happen inside the network
- Reassembly done by end system like in IPv4
- RFC 5722: overlapping fragments => MUST drop the packet. Most OS implement it in 2012
- Attackers can still fragment in intermediate system on purpose ==> a great obfuscation tool

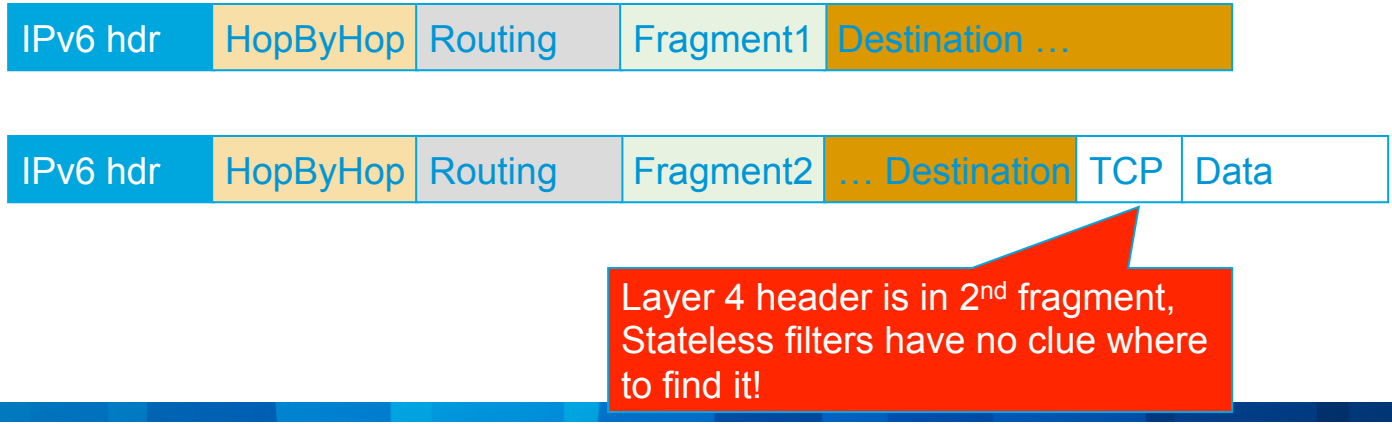


Parsing the Extension Header Chain Fragments and Stateless Filters

- Layer 4 information could be in 2nd fragment
- But, stateless firewalls could not find it if a previous extension header is fragmented
- RFC 3128 is not applicable to IPv6 but

  RFC 6980 *'nodes MUST silently ignore NDP ... if packets include a fragmentation header'* ;-)

  RFC 7112 *'A host that receives a First Fragment that does not satisfy ... SHOULD discard the packet'* ;-)



IPv6 Fragmentation & IOS ACL Fragment Keyword

- This makes matching against the first fragment non-deterministic:
  - layer 4 header might not be there but in a later fragment
  - ⇒Need for stateful inspection
- `fragment` keyword matches
  - Non-initial fragments (same as IPv4)
- `undertermined-transport` keyword does not match
  - If non-initial fragment
  - Or if TCP/UDP/SCTP and ports are in the fragment
  - Or if ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3, RSVP, GRE, ESP, EIGRP, PIM …)
  - Only for deny ACE

RFC 7112 router MAY drop those packets ;-)

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
- Do not confuse 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

NAPT = Network Address and Port Translation

PCI DSS 3.0 Compliance and IPv6

- Payment Card Industry Data Security Standard *(latest revision November 2013)*:

  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)

  …

  the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.

- ➔ 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

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
  - Unprotected without IPsec: sniffing, injection, service stealing
  - Bypass IPv4-only firewalls if badly configured (protocol 41 or UDP)
  - Can cause asymmetric traffic (hence cannot cross stateful devices including firewalls)
  - Should be a thing of the past in 2014

Dual Stack Host Considerations

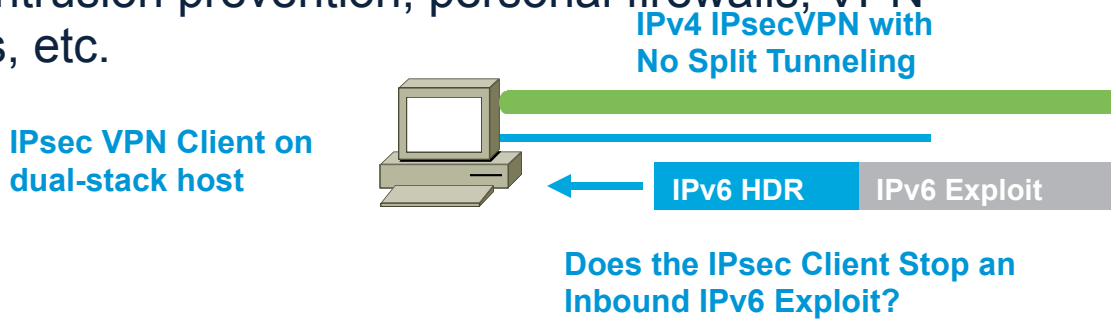
- Host security on a dual-stack device

  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 (Windows7 & 8.x , 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

Enforcing a Security Policy

As an Example: Summary of Cisco IPv6 Security Products

For Your Reference

- 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 and transparent proxy
- Cisco Cloud Web Security (ScanSafe) work in progress (need IPv6 connectivity for all towers...)
- FIREpower NGIPS provides Decoder for IPv4 & IPv6 Packets

Another Example for VPN: Secure IPv6 over IPv4/6 Public Internet

For Your Reference

- No traffic sniffing
- No traffic injection
- No service theft

Public Network	Site 2 Site	Remote Access
IPv4	▪ 6in4/GRE Tunnels Protected by IPsec ▪ DMVPN 12.4(20)T	▪ ISATAP Protected by RA IPsec ▪ SSL VPN Client AnyConnect
IPv6	▪ IPsec VTI 12.4(6)T ▪ DMVPN 15.2(1)T	▪ AnyConnect 3.1 & ASA 9.0

FlexVPN for all use cases

Summary

Key Take Away

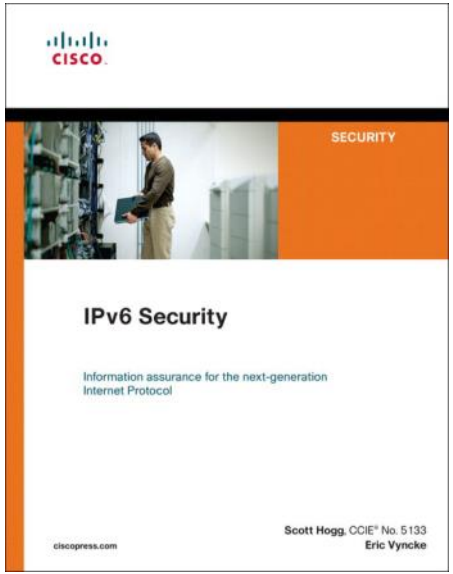
- So, **nothing really new in IPv6**
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - NDP spoofing: RA guard and FHS Features
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them (beware of fragments)
  - Security appliances work for IPv6
- Lack of operation experience may hinder security for a while: **Training is required**
- Security enforcement is possible
  - Control your IPv6 traffic as you do for IPv4
- Leverage IPsec to secure IPv6 when suitable

Is IPv6 in My Network?

- Easy to check!
- Look inside NetFlow records
  - Protocol 41: IPv6 over IPv4 or 6to4 tunnels
  - IPv4 address: 192.88.99.1 (6to4 anycast server)
  - UDP 3544, the public part of Teredo, yet another tunnel
  - ICMPv6 Packets, especially RA
- Check your IPS System for discovery of ICMPv6 Traffic
- Look into DNS server log for resolution of ISATAP & Microsoft Teredo servers
- Beware of the IPv6 latent threat:

Your IPv4-only network may be vulnerable to IPv6 attacks NOW!

Recommended Reading




CISCO