Are we More Secure with IPv6 ?

A quick overview

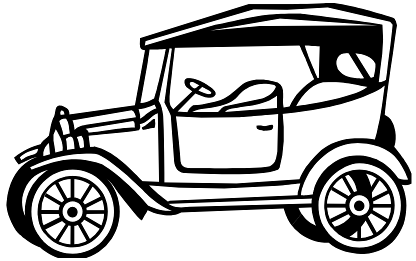
Eric Vyncke evyncke@cisco.com @evyncke
Distinguished Engineer
June 2017

Agenda

- Debunking IPv6 Myths
- Shared Issues by IPv4 and IPv6
- Specific Issues for IPv6
  - Addresses, Extension headers, dual-stack, tunnels
- Summary

IPv6 Security Myths…

IPv6 Myths: Better, Faster, More Secure



Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

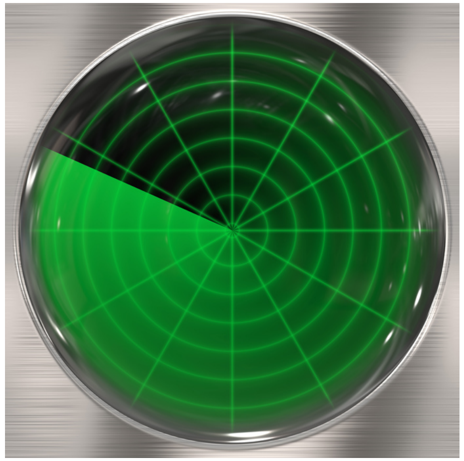
Source: Microsoft clip-art gallery

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...
- RFC 6282 addresses have 16 bits only 0000:00ff:fe00:XXXX
- Using peer-to-peer clients gives IPv6 addresses of peers
- Harvest NTP client addresses by becoming a member of pool.ntp.org
- 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

cisco

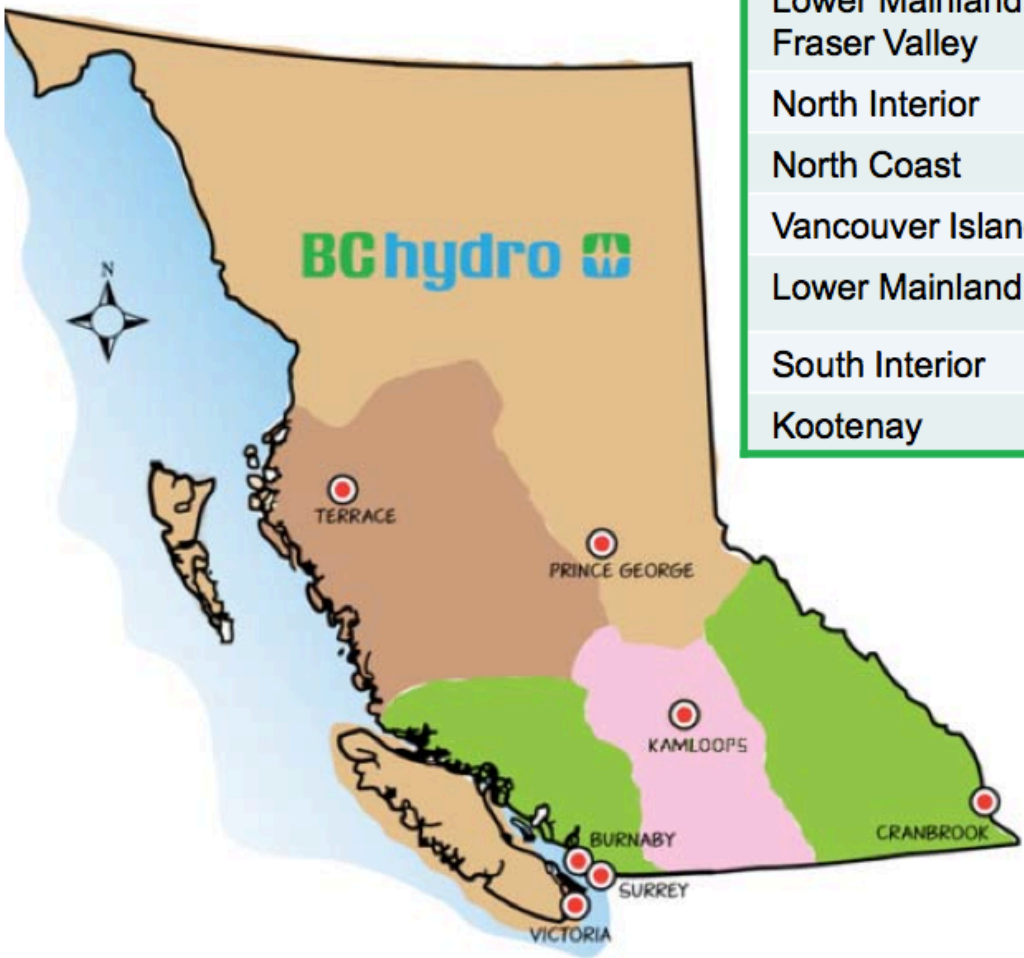
The IPsec Myth: IPsec End-to-End will Save the World

- 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

IoT & Ipsec: Ipsec + IPv6 to 2 millions meters



Area	Cross-Dock	Total
Lower Mainland South – Fraser Valley	Surrey	444,224
North Interior	Prince George	104,362
North Coast	Terrace	42,430
Vancouver Island	Victoria	387,898
Lower Mainland Metro	Burnaby	623,627
South Interior	Kamloops	191,965
Kootenay	Cranbrook	54,433

TOTAL 1,848,939

8

Comparing Pre-IPv6 to Full IPv6 After Conversion

	Pre-IPV6			Post IPV6	
	CE ping (sec) Avg of 3 node pings (C12.22)[1]	DIFF (ms) between levels		AVG (ms) round-trip CGR to meter (ICMP)[2]	DIFF (ms) between levels
CGR	2.67				
L1	4.0	1,330		430.5	
L2	5.0	1,000		716.1	285.7
L3	7.33	2,330		1,074	357.5
L4	8.33	1,000		1,119	45.05
L5	11.33	3,000			
Average		**1,732**			**279.69**

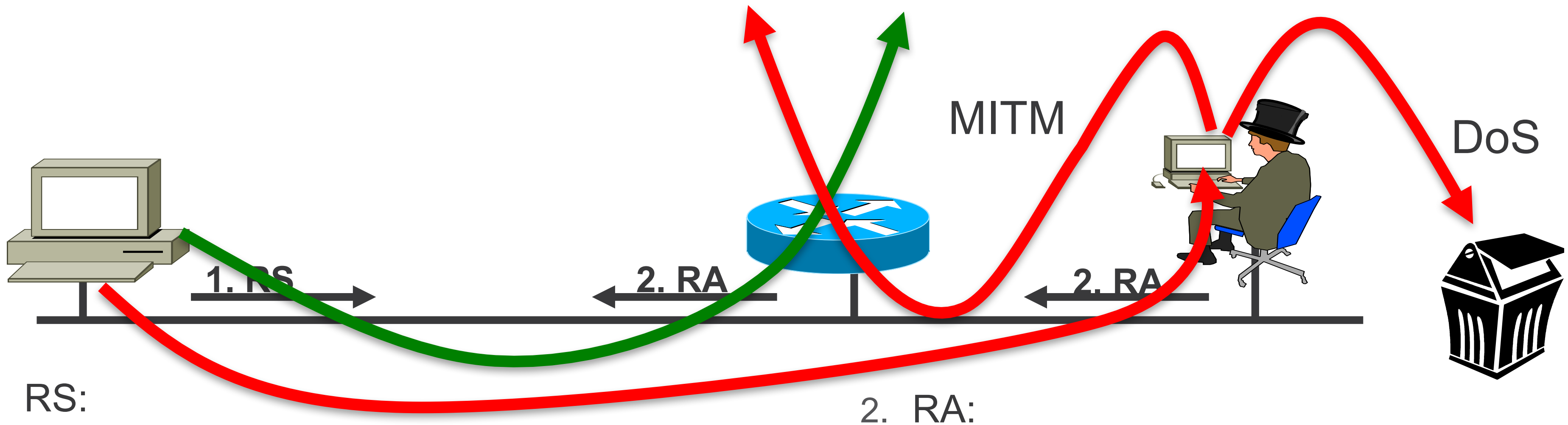
[1] C12.22 message protocol from collection engine
[2] ICMP ping

Shared Issues

StateLess Address Auto Configuration SLAAC Rogue Router Advertisement

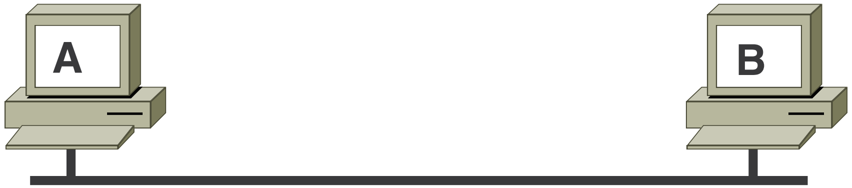
- **Router Advertisements (RA)** contains:
  - Prefix to be used by hosts
  - Data-link layer address of the router
  - Miscellaneous options: MTU, DHCPv6 use, …

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

Neighbor Solicitation



Src = A
Dst = Solicited-node multicast of B
ICMP type = 135
Data = link-layer address of A
Query: what is your link address?

Src = B
Dst = A
ICMP type = 136
Data = link-layer address of B

A and B Can Now Exchange Packets on This Link

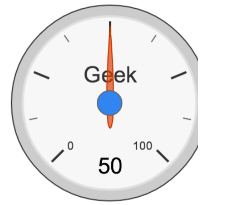
Security Mechanisms Built into Discovery Protocol = None

Last Come is Used

=> Very similar to ARP

Attack Tool from THC: Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...

ARP Spoofing is now NDP Spoofing: Mitigation



- **GOOD NEWS**: First-Hop-Security for IPv6 is available
  - IETF SAVI WG: RA guard, DHCP guard, …
  - IEEE 802.15.4 and other IoT layer-2 network have some crypto protections
  - 6LoWPAN can have a large layer-2 span => specific mechanism
- **(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)

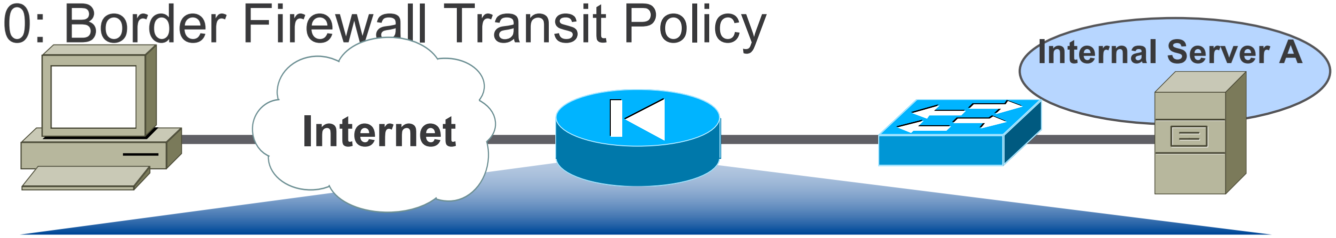
ICMPv4 vs. ICMPv6

- Significant changes
- More relied upon
- => ICMP policy on firewalls

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

Equivalent ICMPv6

RFC 4890: Border Firewall Transit Policy

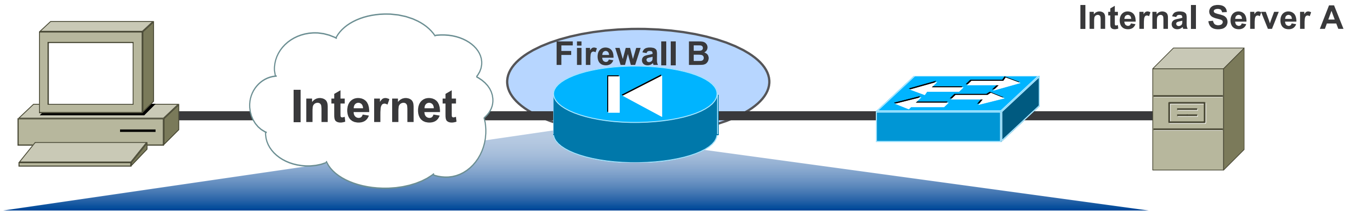


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	Unreachable
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—HL Exceeded
Permit	Any	A	4	0	Parameter Problem

Needed for Teredo traffic

Potential Additional ICMPv6

RFC 4890: Border Firewall Transit 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

Remote NDP Floods...

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160525-ipv6 (May 2016)
- http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-01-ipv6-en (August 2016)
- https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10749 (September 2016)
- RFC 4890 is a little too open

Permi	Any	B	135/136	0	Neighbor Solicitation and Advertisement

- RFC 4861 (Neighbor Discovery)
  - Hop Limit MUST be 255
  - Source should be link-local, unspecified or global address belonging to the link and not "any"

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

Good news
IPv4 IPS
signatures can be
re-used

cisco

Specific IPv6 Issue #1
Addresses

Multiple Facets to IPv6 Addresses

- Every host can have multiple IPv6 addresses simultaneously
  - Need to do correlation!
  - Alas, no Security Information and Event Management (SIEM) supports IPv6
  - Usually, a customer is identified by its /48 ☺
- Every IPv6 address can be written in multiple ways
  - 2001:0DB8:0BAD::0DAD
  - 2001:DB8:BAD:0:0:0:0:DAD
  - 2001:db8:bad::dad (this is the canonical RFC 5952 format)
  - => Grep cannot be used anymore to sieve log files…

Link-Local Addresses vs. Global Addresses

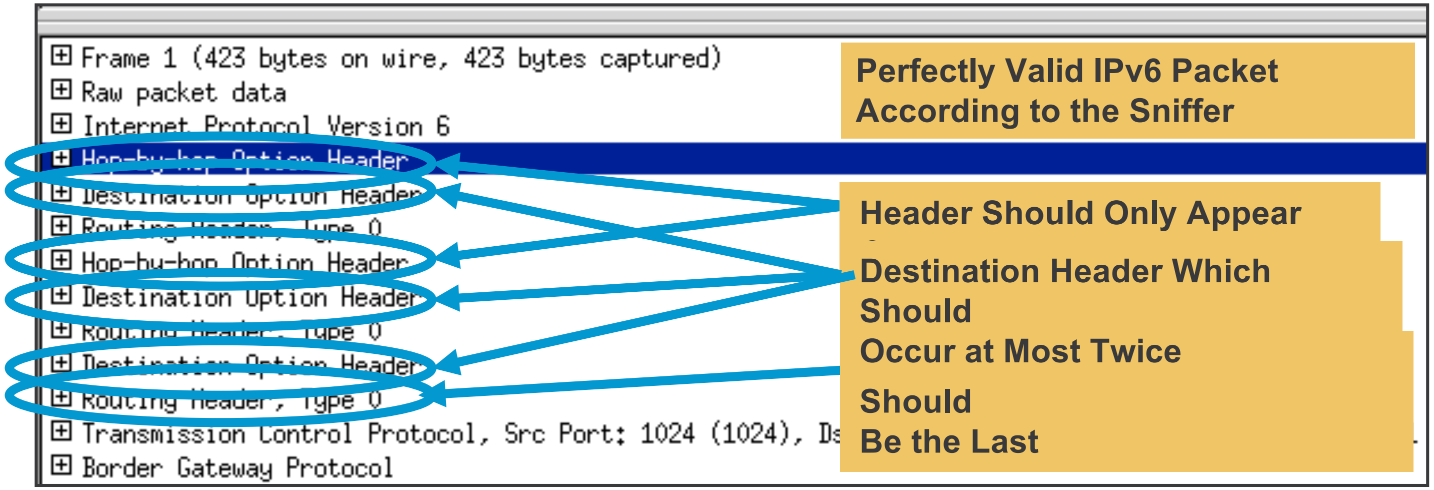
- Link-Local addresses, fe80::/16, (LLA) are isolated
  - Cannot reach outside of the link
  - **Cannot be reached from outside of the link ☺**
- Could be used on the infrastructure interfaces
  - Routing protocols (inc BGP) work with LLA
  - Benefit: no remote attack against your infrastructure
  - Implicit infrastructure ACL
  - *See also: RFC7404*

cisco

Specific IPv6 Issue #2
Extension Headers

IPv6 Header Manipulation

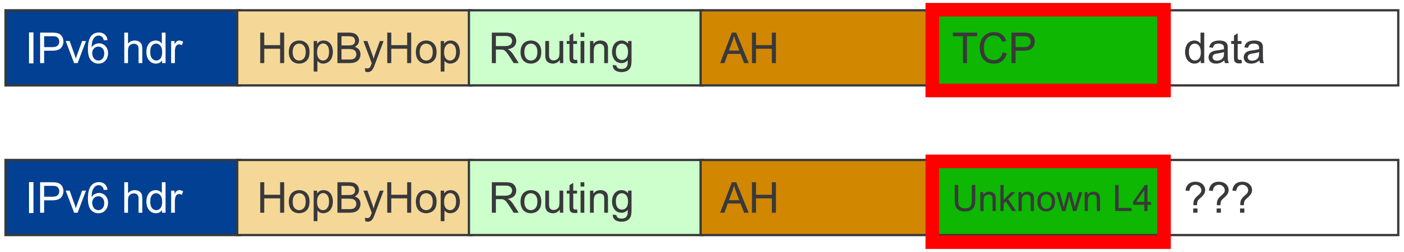
- Unlimited size of header chain (spec-wise) can make filtering difficult
- Potential DoS with poor IPv6 stack implementations
    - More boundary conditions to exploit
    - Can I overrun buffers with a lot of extension headers?
    - Mitigation: a firewall such as ASA which can filter on headers



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

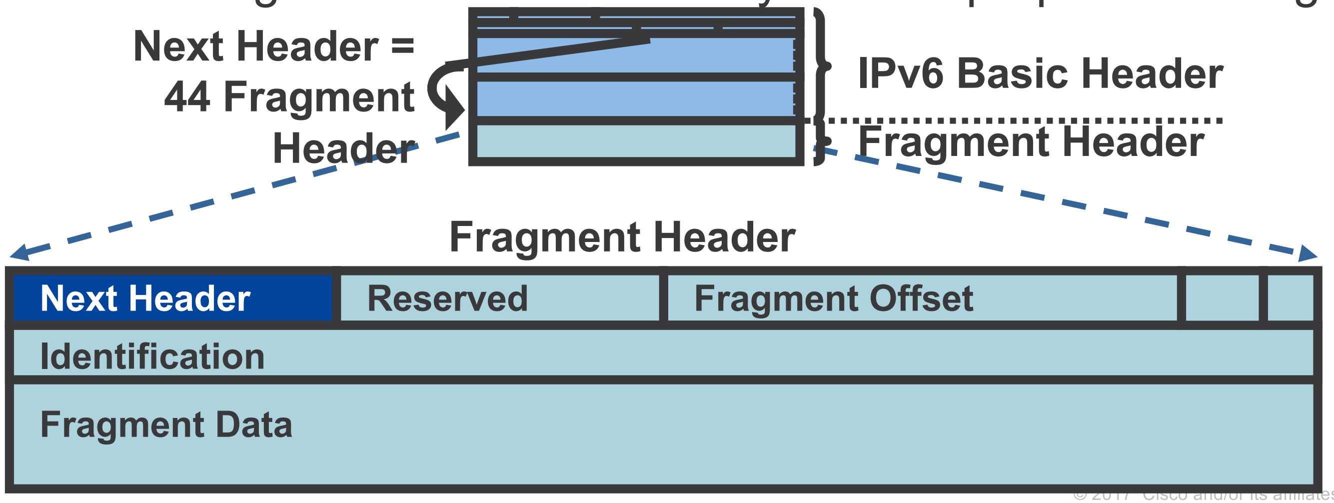
Parsing the Extension Header Chain

- 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**



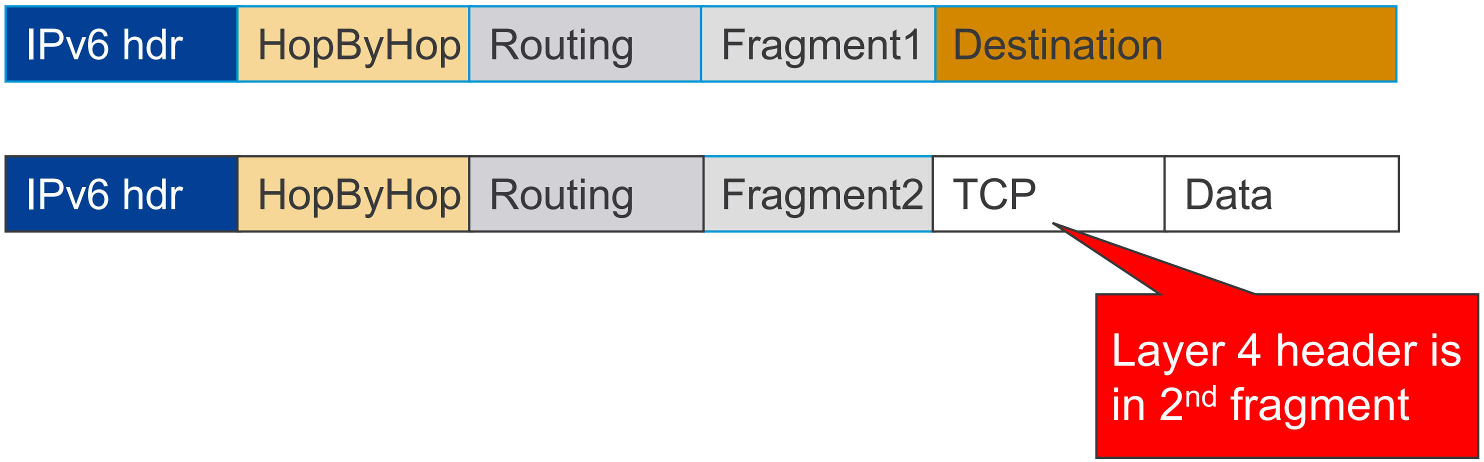
Fragment Header: IPv6

- 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



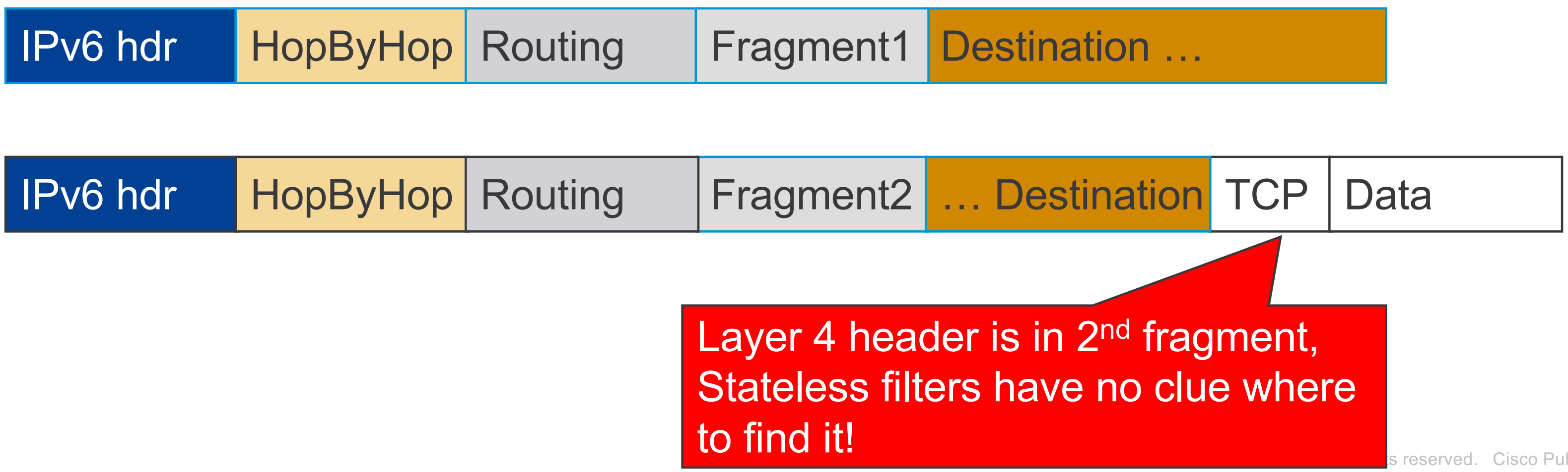
Parsing the Extension Header Chain Fragmentation Matters!

- Extension headers chain can be so large than it must be fragmented!
- RFC 3128 is not applicable to IPv6
- Layer 4 information could be in 2nd fragment



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'* ;-)

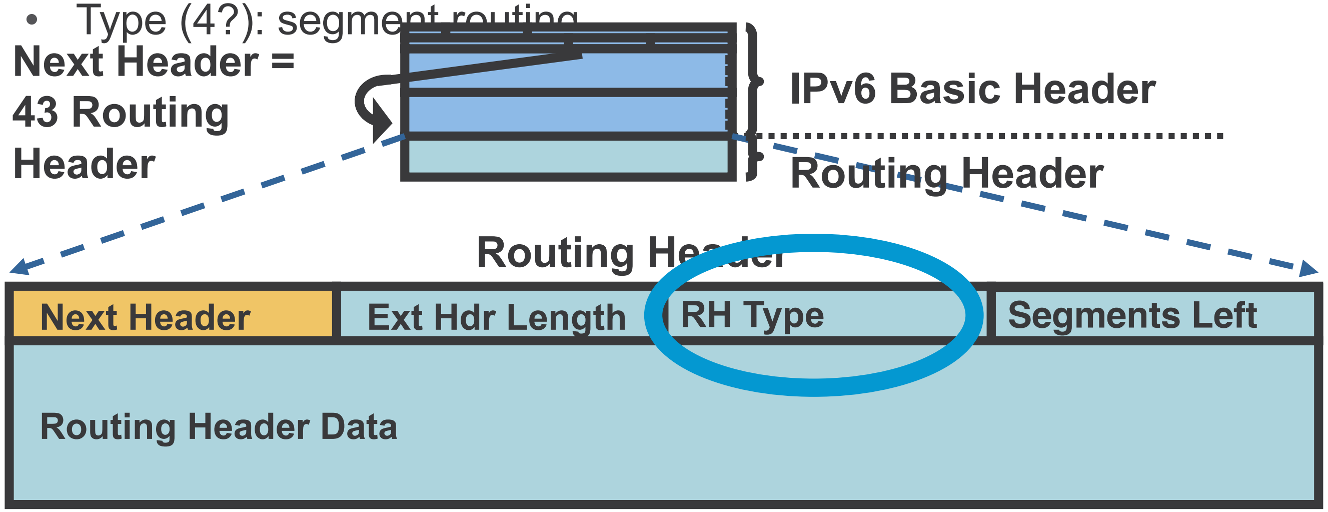


Is it the End of the World?

- The lack of fast wirespeed stateless ACL is a bad news of course
- IETF made 1st IPv6 fragment without layer-4 invalid and it SHOULD be dropped by receiving host and MAY be dropped by routers
  - RFC 7112 (born as draft-ietf-6man-oversized-header-chain)

IPv6 Routing Header

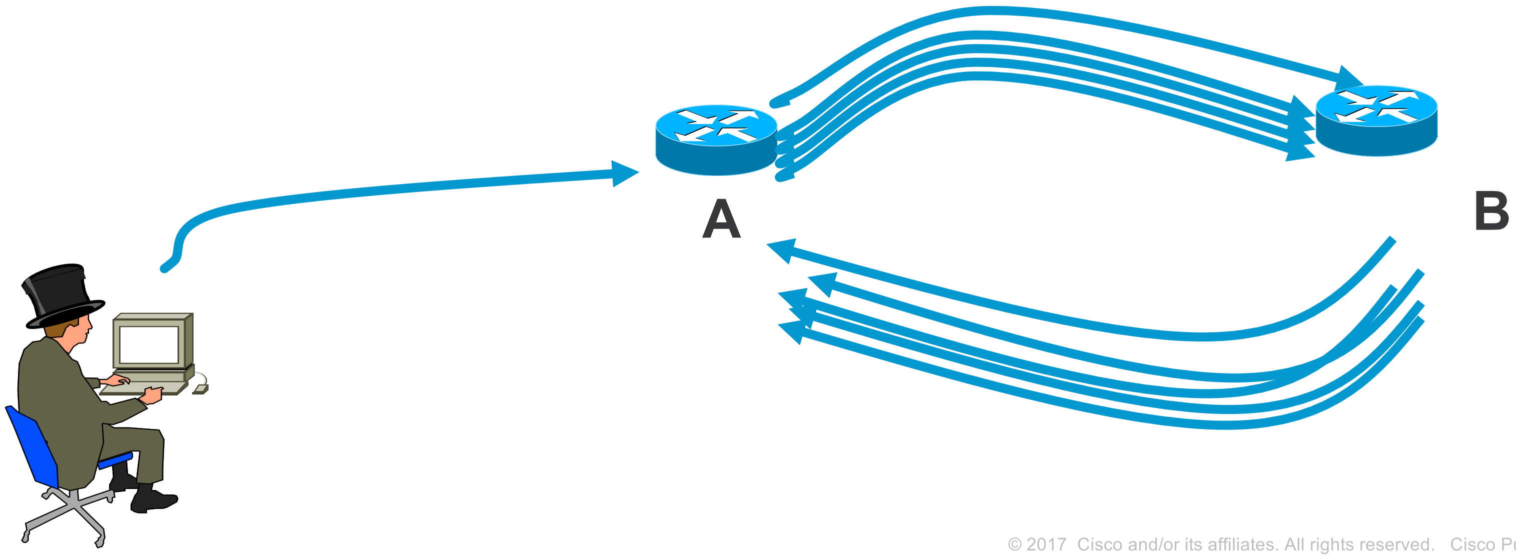
- Processed by intermediate routers
- Three types
  - Type 0: similar to IPv4 source routing (multiple intermediate routers)
  - Type 2: used for mobile IPv6
  - Type 3: used by RPL (Routing Protocol for Low-Power and Lossy Networks)
  - Type (4?): segment routing



Routing Header Type 0

Amplification Attack

- What if attacker sends a packet with RH containing
  - A -> B -> A -> B -> A -> B -> A -> B -> A ....
- Packet will loop multiple time on the link A-B
- An amplification attack!

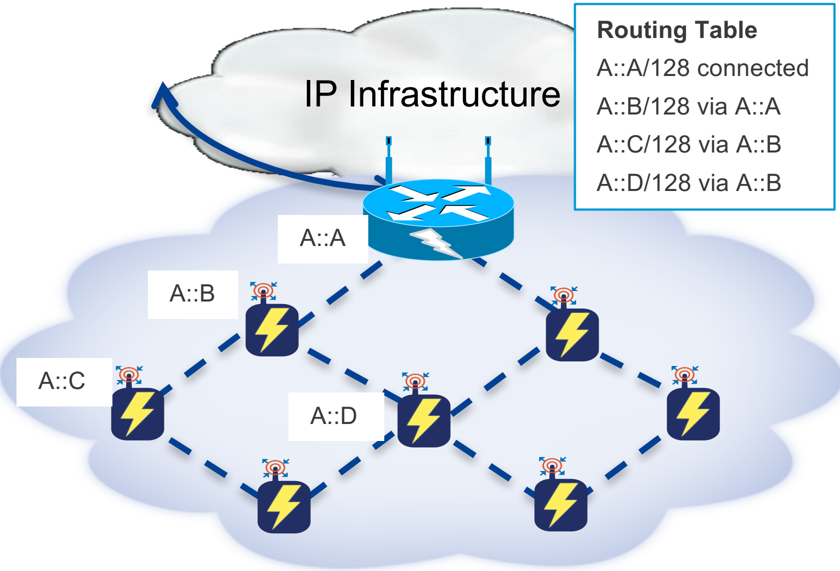


Preventing Routing Header-0 Attacks

- RFC 5095 (Dec 2007) RH-0 is deprecated
- Type 2 and type 3 (+SR – type 4) are not dangerous and should be allowed

Routing Header Type 3 for RPL is OK

- Used by Routing Protocol for Low-Power and Lossy Networks
- But only within a single trusted network (strong authentication of node), never over a public untrusted network
  - Damage is limited to this RPL network
  - If attacker is inside the RPL network, then he/she could do more damage anyway



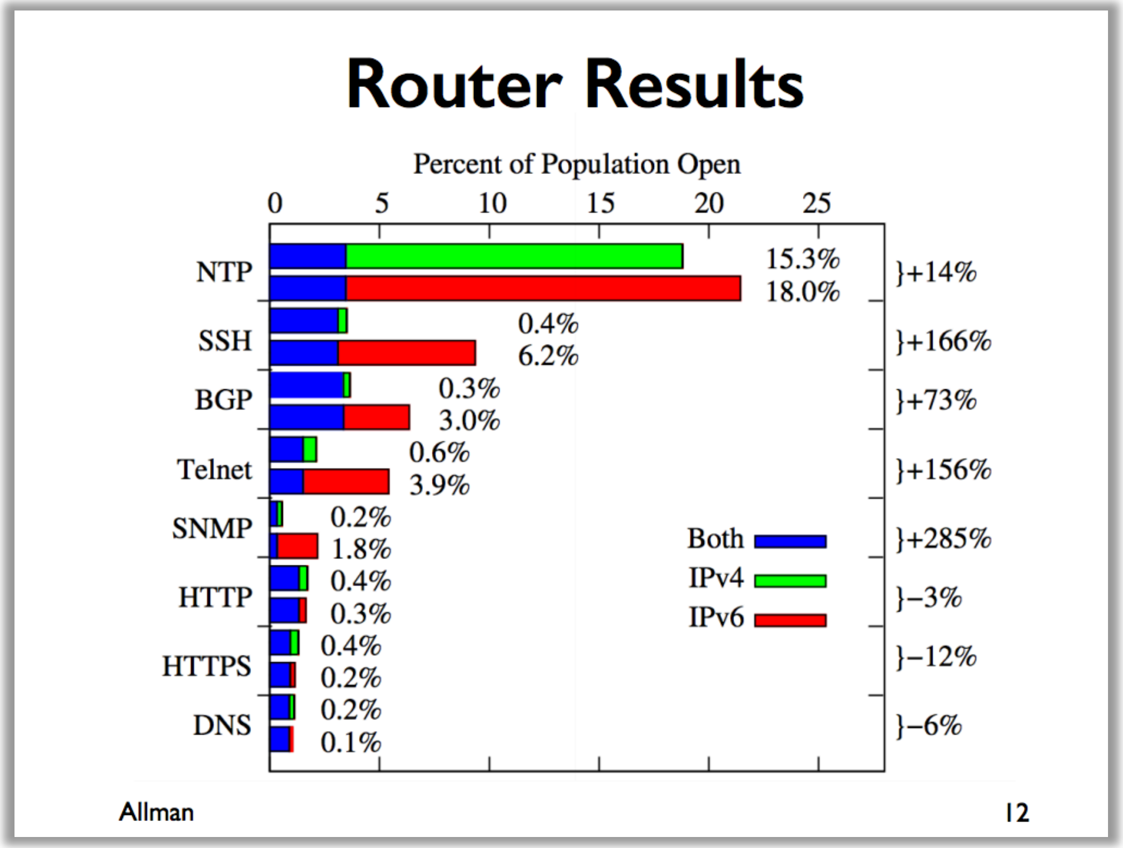
Specific IPv6 Issue #3 Dual-Stack Network

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.

Non-Congruent Security Policies ☹

- Test done in 2016 on 25K routers
- SSH is more open in IPv6 (9%) than IPv4 (4%)
- Telnet is more open in IPv6 (6%) than in IPv4 (3%)



https://www.ietf.org/proceedings/95/slides/slides-95-maprg-0.pdf (Mark Allman)

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

More IPv6 Specifics

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

"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

Using SNMP to Read IPv4/IPv6 Neighbors Cache


```
evyncke@charly:~$ snmpwalk -c secret -v 1 udp6:[2001:db8::1] -m IP-MIB
ipNetToPhysicalPhysAddress

IP-MIB::ipNetToPhysicalPhysAddress.1.ipv4."192.168.0.2" = STRING: 0:13:c4:43:cf:e

IP-MIB::ipNetToPhysicalPhysAddress.1.ipv4."192.168.0.3" = STRING: 0:23:48:2f:93:24

IP-MIB::ipNetToPhysicalPhysAddress.1.ipv4."192.168.0.4" = STRING: 0:80:c8:e0:d4:be

...

IP-MIB::ipNetToPhysicalPhysAddress.2.ipv6."2a:02:05:78:85:00:01:01:02:07:e9:ff:fe:f2:a0:c6" =
STRING: 0:7:e9:f2:a0:c6

IP-MIB::ipNetToPhysicalPhysAddress.2.ipv6."2a:02:05:78:85:00:01:01:02:20:4a:ff:fe:bf:ff:5f" =
STRING: 0:20:4a:bf:ff:5f

IP-MIB::ipNetToPhysicalPhysAddress.2.ipv6."2a:02:05:78:85:00:01:01:30:56:da:9d:23:91:5e:ea" =
STRING: 78:ca:39:e2:43:3

...

evyncke@charly:~$ snmptable -c secret -v 1 udp6:[2001:db8::1] -Ci -m IP-MIB
ipNetToPhysicalTable
```

For Your Reference

IPFIX Record: IPv6 Key Fields

IPv6	
IP (Source or Destination)	Payload Size
Prefix (Source or Destination)	Packet Section (Header)
Mask (Source or Destination)	Packet Section (Payload)
Minimum-Mask (Source or Destination)	DSCP
Protocol	Extension
Traffic Class	Hop-Limit
Flow Label	Length
Option Header	Next-header
Header Length	Version
Payload Length	

Routing
Destination AS
Peer AS
Traffic Index
Forwarding Status
Is-Multicast
IGP Next Hop
BGP Next Hop

Flow
Sampler ID
Direction

Interface
Input
Output

Transport	
Destination Port	TCP Flag: ACK
Source Port	TCP Flag: CWR
ICMP Code	TCP Flag: ECE
ICMP Type	TCP Flag: FIN
IGMP Type	TCP Flag: PSH
TCP ACK Number	TCP Flag: RST
TCP Header Length	TCP Flag: SYN
TCP Sequence Number	TCP Flag: URG
TCP Window-Size	UDP Message Length
TCP Source Port	UDP Source Port
TCP Destination Port	UDP Destination Port
TCP Urgent Pointer	

Flexible Flow Record: IPv6 Extension Header Map

Bits 11-31	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Res	ESP	AH	PAY	DST	HOP	Res	UNK	FRA0	RH	FRA1	Res

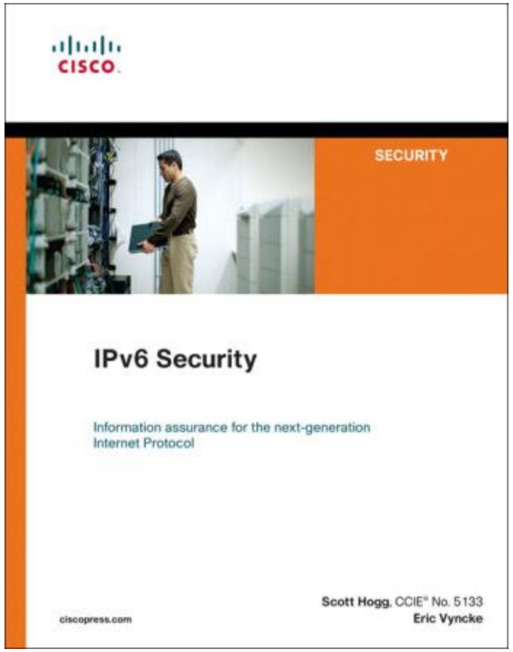
- FRA1: Fragment header – not first fragment
- **RH: Routing header**
- FRA0: Fragment header – First fragment
- UNK: Unknown Layer 4 header (compressed, encrypted, not supported)
- **HOP: Hop-by-hop extension header**
- DST: Destination Options extension header
- PAY: Payload compression header
- AH: Authentication header
- ESP: Encapsulating Security Payload header
- Res: Reserved

Summary

Key Take Away

- So, **nothing really new in IPv6**
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - NDP spoofing: RA guard and FHS Features
  - ICMPv6 firewalls need to change policy to allow NDP
  - Extension headers: firewall & ACL can process them
- 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

Recommended Reading



OPSEC — K. Chittimaneni
Internet-Draft — Dropbox Inc.
Intended status: Informational — M. Kaeo
Expires: October 13, 2017 — Double Shot Security
E. Vyncke, Ed.
Cisco
April 11, 2017

Operational Security Considerations for IPv6 Networks
draft-ietf-opsec-v6-11

More on www.ciscolive.com (free but required registration)