IPv6 Security

A quick overview

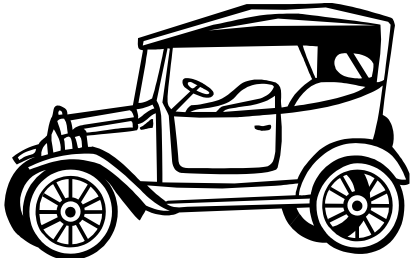
Eric Vyncke evyncke@cisco.com @evyncke
Distinguished Engineer
June 2017

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!

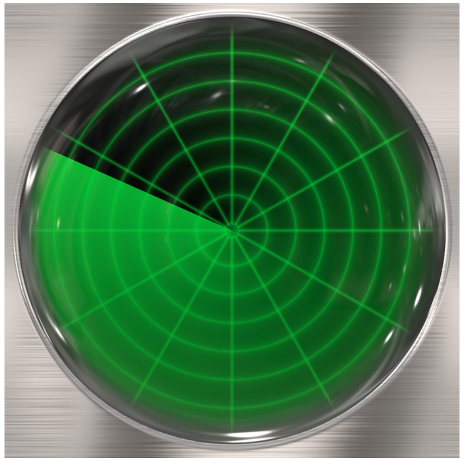
Source: Microsoft clip-art gallery

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

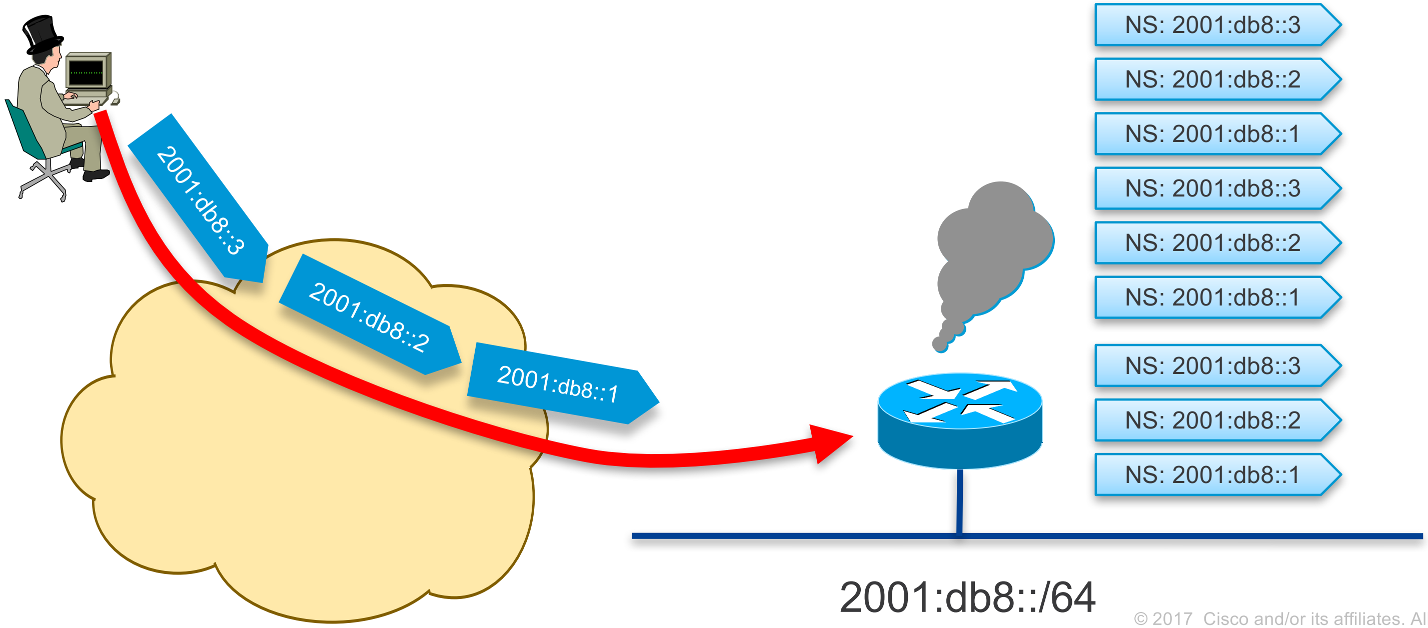


Source: Microsoft clip-art gallery

- 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...
- Increased deployment/reliance on dynamic DNS
  - More information will be in DNS
- 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

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/…



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 ?

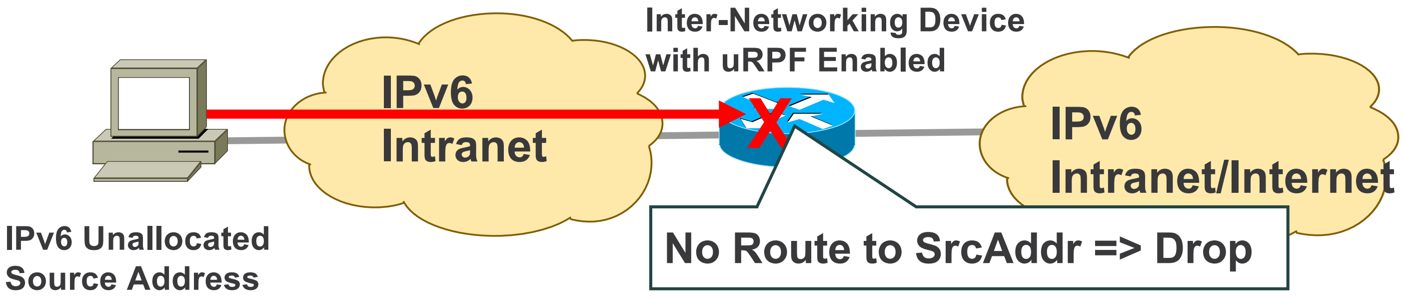
Recommendation: do not use IPsec end to end within an administrative domain.

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

Shared Issues

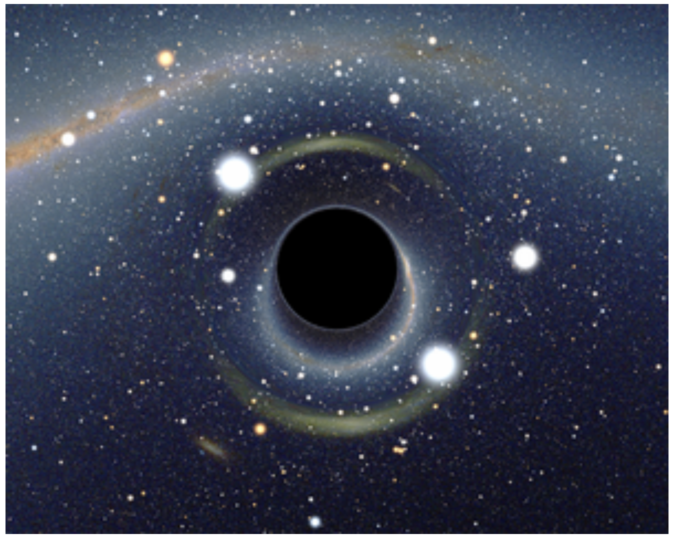
IPv6 Bogon and Anti-Spoofing Filtering

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



Remote Triggered Black Hole

- RFC 5635 RTBH is as easy in IPv6 as in IPv4
- uRPF is also your friend for black holing a source
- RFC 6666 has a specific discard prefix
  - 100::/64



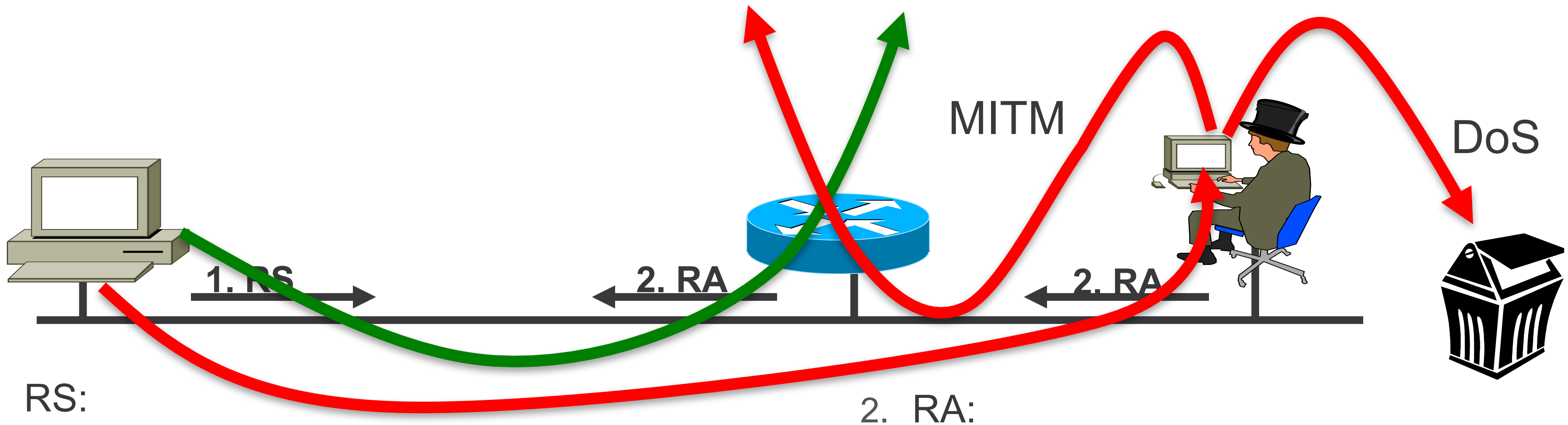
Source: Wikipedia Commons

- http://www.cisco.com/web/about/security/intelligence/ipv6_rtbh.html

Neighbor Discovery Issue#1 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, …

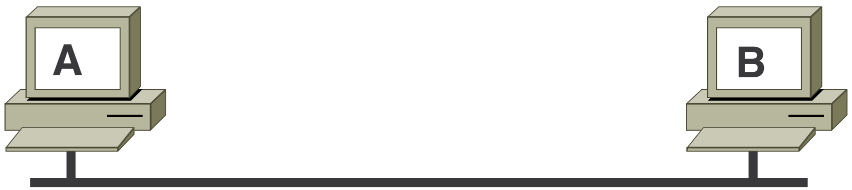
RA w/o Any Authentication Gives Exactly Same Level of Security as DHCPv4 (None)



1. RS:
   - Data = Query: please send RA

2. RA:
   - Data= options, prefix, lifetime, A+M+O flags

Neighbor Discovery Issue#2
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

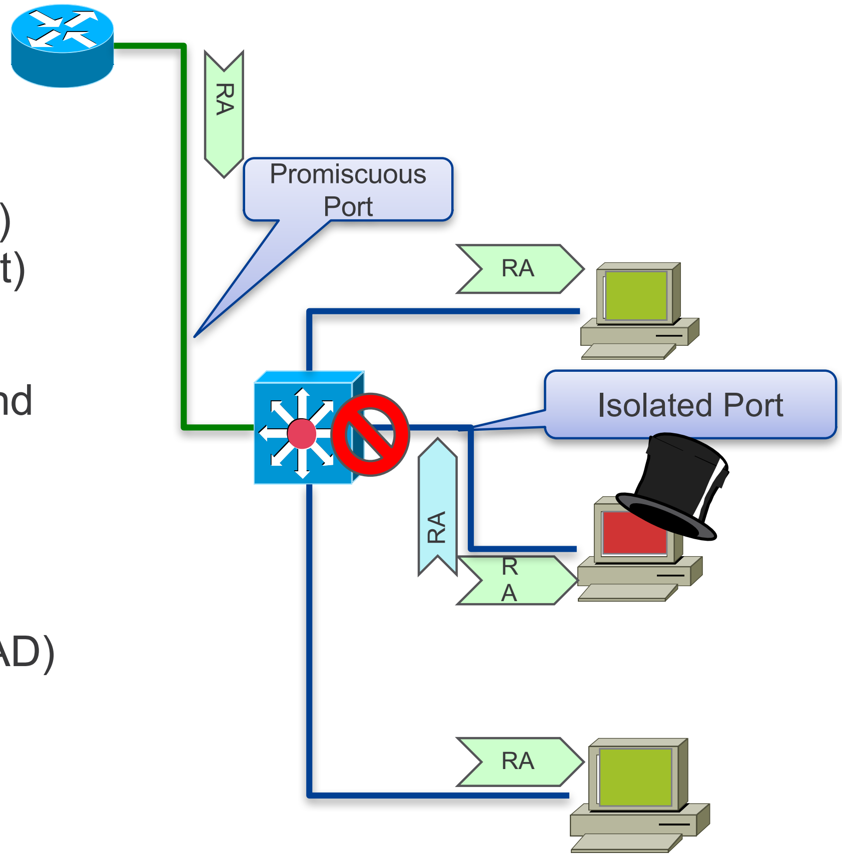
Attack Tool from THC: Parasite6
Answer to all NS, Claiming to Be All Systems in the LAN...

ARP Spoofing is now NDP Spoofing: Mitigation

- **GOOD NEWS**: First-Hop-Security for IPv6 is available
  - 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

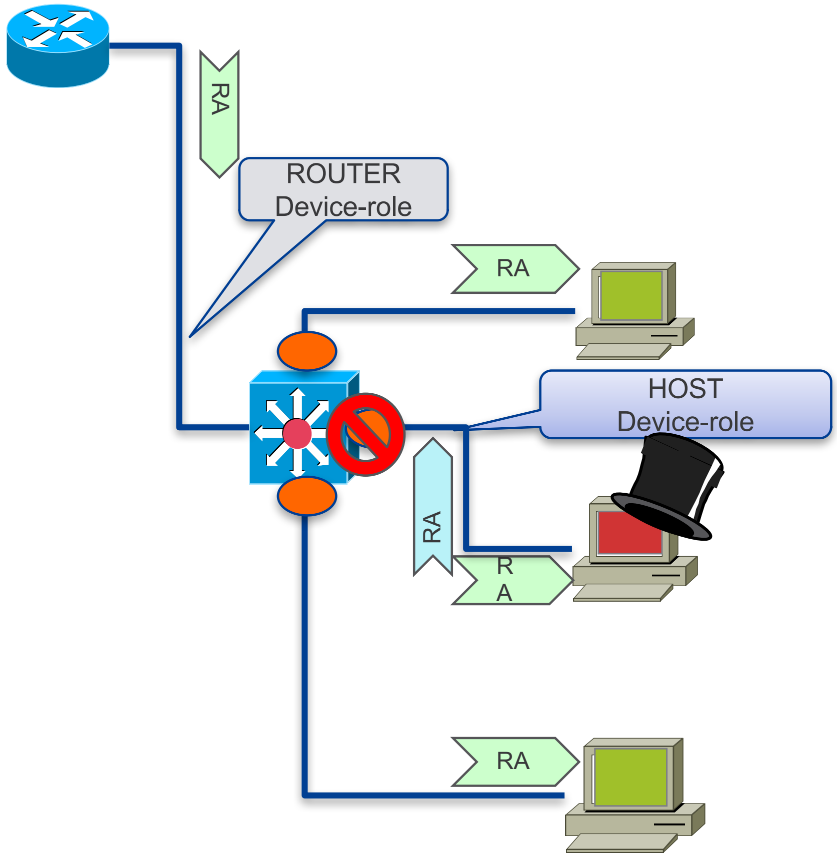
```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- **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
```



ICMPv4 vs. ICMPv6

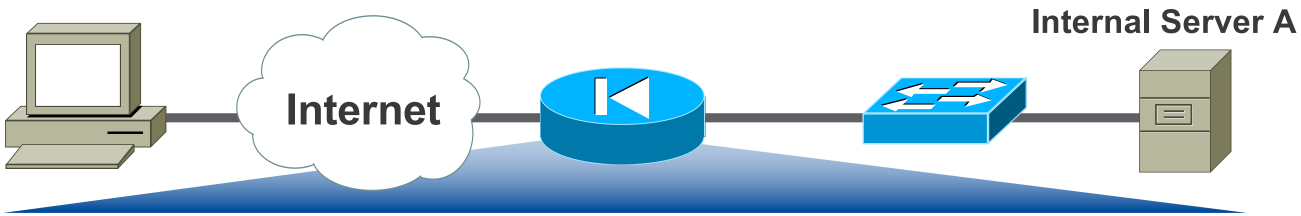
- Significant changes
- More relied upon

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

Generic ICMPv4

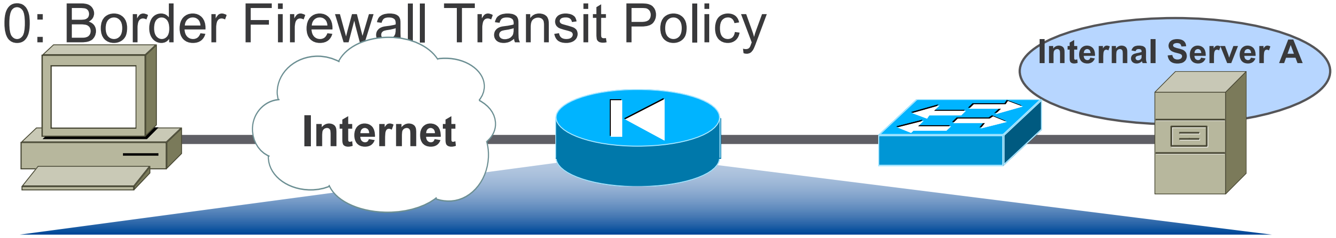
Border Firewall Policy



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

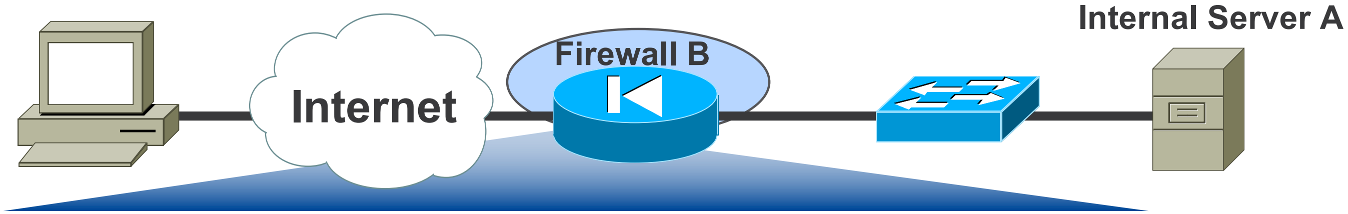


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	A	128	0	Echo Reply
Permit	Any	A	129	0	Echo Request
Permit	Any	A	1	0	Unreachable
Permit	Any	A	2	0	Packet Too Big
Permit	Any	A	3	0	Time Exceeded—HL Exceeded
Permit	Any	A	4	0	Parameter Problem

Needed for Teredo traffic

Potential Additional ICMPv6

RFC 4890: Border Firewall Transit Policy

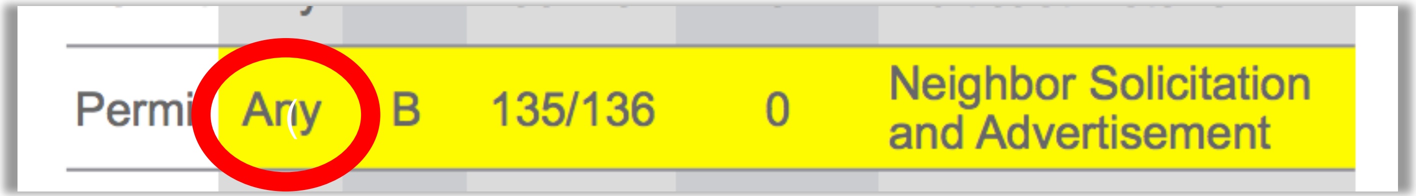


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	135/136	0	Neighbor Solicitation and Advertisement
Deny	Any	Any			

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



- 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"

Preventing IPv6 Routing Attacks

Protocol Authentication

- BGP, ISIS, EIGRP no change:
  - An MD5 authentication of the routing update
- OSPFv3 has changed and pulled MD5 authentication from the protocol and instead rely on transport mode IPsec (for authentication and **confidentiality**)
  - But see RFC ~~6506~~ 7166 *(but not widely implemented yet)*
- IPv6 routing attack best practices
  - Use traditional authentication mechanisms on BGP and IS-IS
  - Use IPsec to secure protocols such as OSPFv3

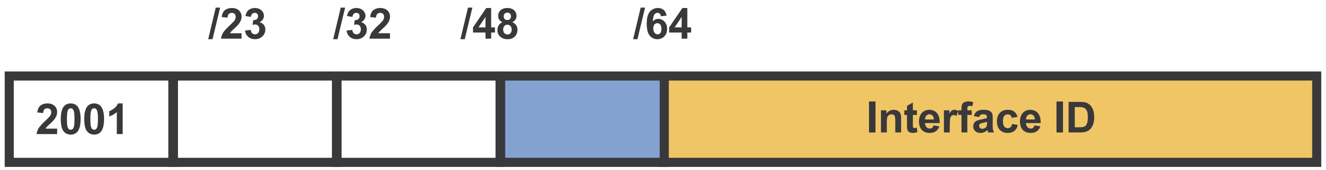
IPv6 Attacks with Strong IPv4 Similarities

- 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

Specific IPv6 Issue #1 Addresses

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)

Disabling Privacy Extension

- Alternatively 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

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

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

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…

Perl to Canonical IPv6 Addresses


```perl
#!/usr/bin/perl -w
use strict ;
use Socket ;
use Socket6 ;

my (@words, $word, $binary_address) ;

## go through the file one line at a time
while (my $line = <STDIN>) {
      @words = split /[ \n]/, $line ;
      foreach $word (@words) {
            $binary_address = inet_pton AF_INET6, $word ;
            if ($binary_address) {
                  print inet_ntop AF_INET6, $binary_address ;
            } else {
                  print $word ;
            }
            print " " ;
      }
      print "\n" ;
}
```

How to Find the MAC Address of an IPv6 Address?

- Easy if EUI-64 format as MAC is embedded
  - 2001:db8::0226:bbff:fe4e:9434
    - *(need to toggle bit 0x20 in the first MAC byte = U/L)*
  - Is 00:26:bb:4e:94:34

How to Find the MAC Address of an IPv6 Address?

- DHCPv6 address or prefix… the client DHCP Unique ID (DUID) can be
  - MAC address: trivial
  - Time + MAC address: simply take the last 6 bytes
  - Vendor number + any number: no luck… next slide can help
  - No guarantee of course that DUID includes the real MAC address.

```
# show ipv6 dhcp binding
Client: FE80::225:9CFF:FEDC:7548
  DUID: 000100010000000A00259CDC7548
  Username : unassigned
  Interface : FastEthernet0/0
  IA PD: IA ID 0x0000007B, T1 302400, T2 483840
    Prefix: 2001:DB8:612::/48
            preferred lifetime 3600, valid lifetime 3600
            expires at Nov 26 2010 01:22 PM (369)
```

DHCPv6 in Real Live…

Geek 0 50 100

- Not so attractive ☹
- Only supported in Windows Vista, and Windows 7, Max OS/X Lion
  - Not in Linux (default installation), …
- Windows Vista does not place the used MAC address in DUID but any MAC address of the PC
- See also: https://knowledge.zomers.eu/misc/Pages/How-to-reset-the-IPv6-DUID-in-Windows.aspx

```
# show ipv6 dhcp binding
Client: FE80::FDFA:CB28:10A9:6DD0
  DUID: 0001000110DB0EA6001E33814DEE
  Username : unassigned
  IA NA: IA ID 0x1000225F, T1 300, T2 480
    Address: 2001:DB8::D09A:95CA:6918:967
            preferred lifetime 600, valid lifetime 600
            expires at Oct 27 2010 05:02 PM (554 seconds)
```

Actual MAC address: 0022.5f43.6522

RADIUS Accounting with IEEE 802.1X (WPA)

- Interesting attribute: **`Acct-Session-Id`** to map username to IPv6 addresses
- Can be sent at the begin and end of connections
- Can also be sent periodically to capture privacy addresses
- Not available through GUI, must use CLI to configure

```
config wlan radius_server acct framed-ipv6 both
```

```
username=joe@example.org Acct-Session-Id=xyz Acct-Status-Type=Start
Framed-IP-Address=192.0.2.1 Framed-IPv6-Address=fe80::cafe

username=joe@example.org Acct-Session-Id=xyz Acct-Status-Type=Alive
Framed-IP-Address=192.0.2.1 Framed-IPv6-Address=fe80::cafe Framed-IPv6-
Address=2001:db8::cafe Framed-IPv6-Address=2001:db8::babe

username=joe@example.org Acct-Session-Id=xyz Acct-Status-Type=Stop Framed-
IP-Address=192.0.2.1
```

How to Find the MAC Address of an IPv6 Address?

- Last resort… look in the live NDP cache (CLI or SNMP)

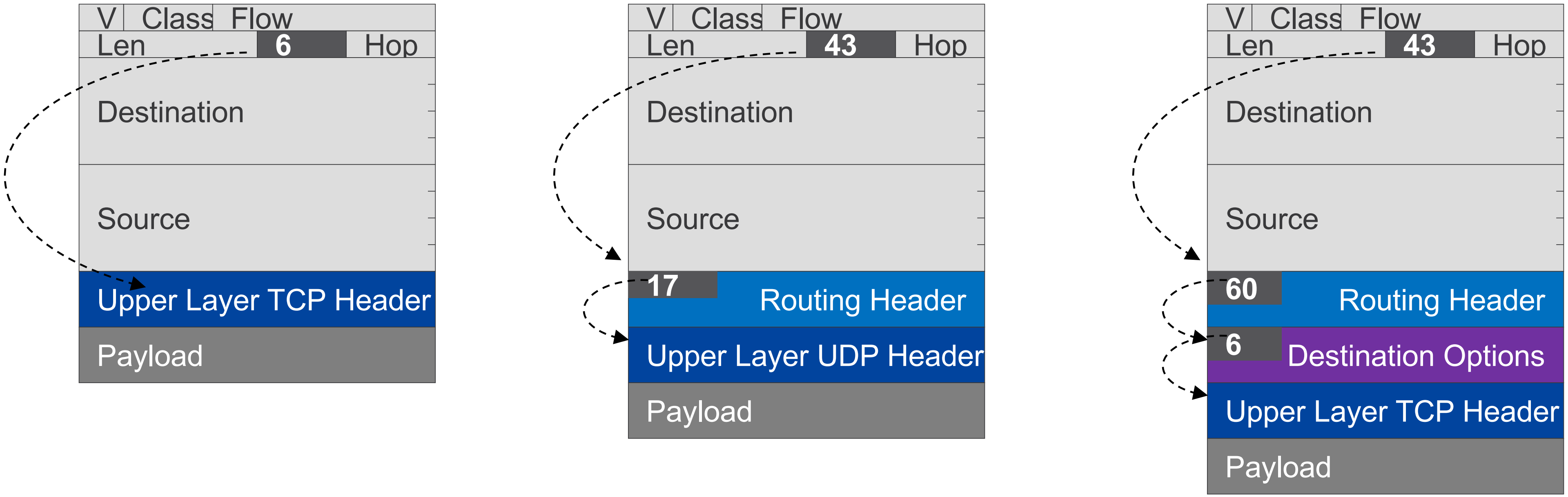
```
#show ipv6 neighbors 2001:DB8::6DD0
IPv6 Address      Age Link-layer Addr State Interface

2001:DB8::6DD0      8 0022.5f43.6522  STALE Fa0/1
```

- If no more in cache, then you should have scanned and saved the cache…
- EEM can be your friend
- First-Hop Security can generate a syslog event on each new binding
  - `ipv6 neighbor binding logging`

Specific IPv6 Issue #2
Extension Headers

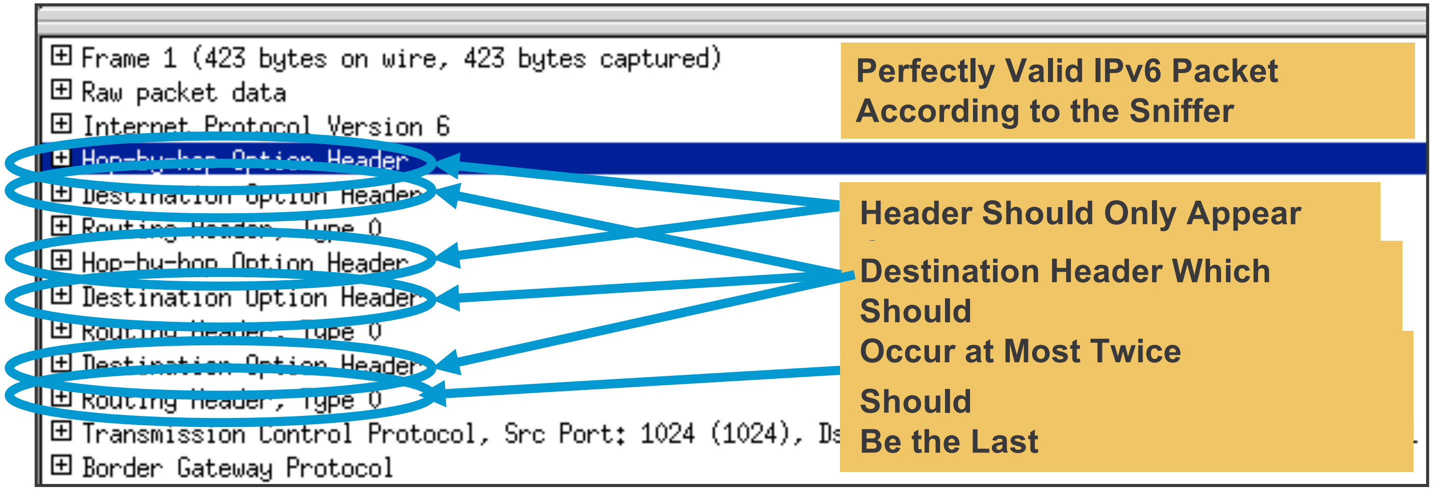
Extension Headers



- Extension Headers Are Daisy Chained
- Upper Layer Headers, must be last, following extension headers

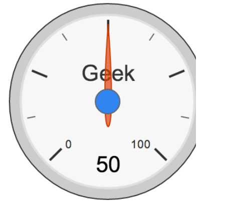
IPv6 Header Manipulation

- 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

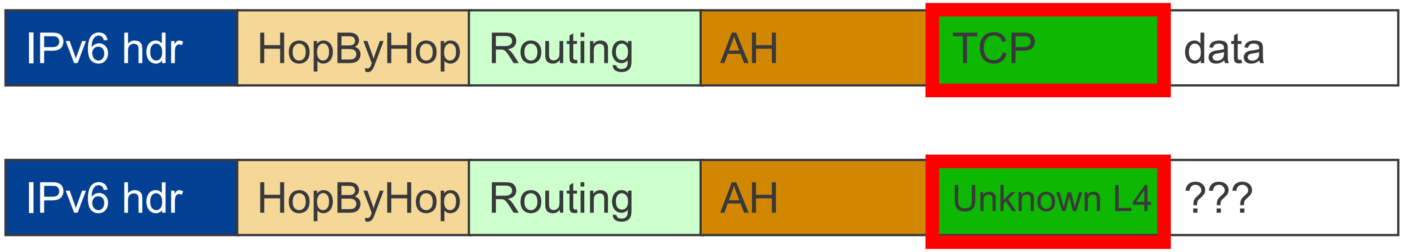


http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Parsing the Extension Header Chain

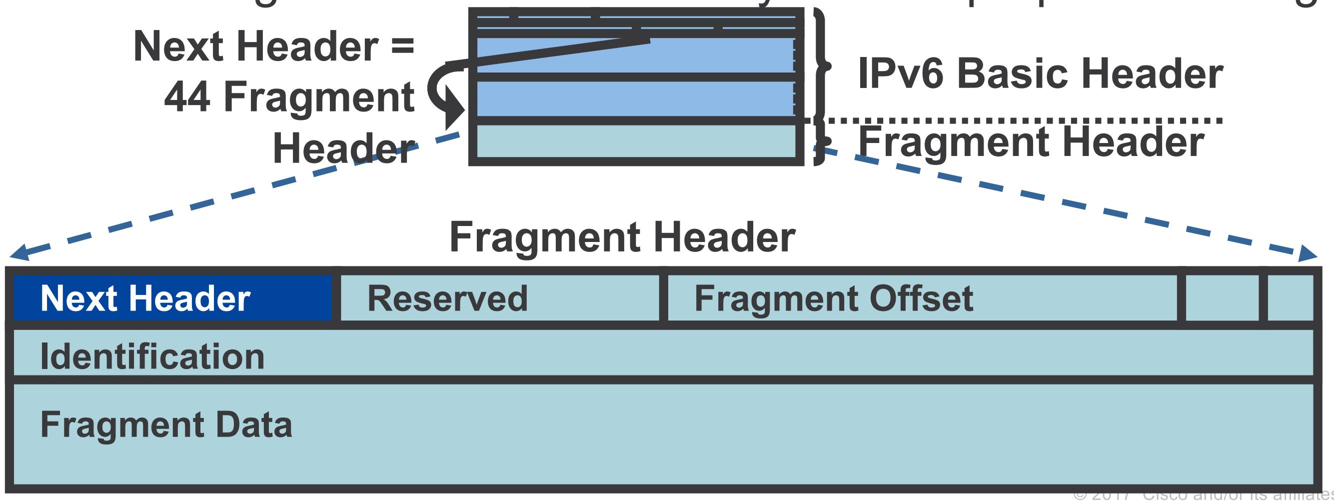


- Finding the layer 4 information is not trivial in IPv6
  - Skip all known extension header
  - Until either known layer 4 header found => **MATCH**
  - Or unknown extension header/layer 4 header found... => **NO MATCH**



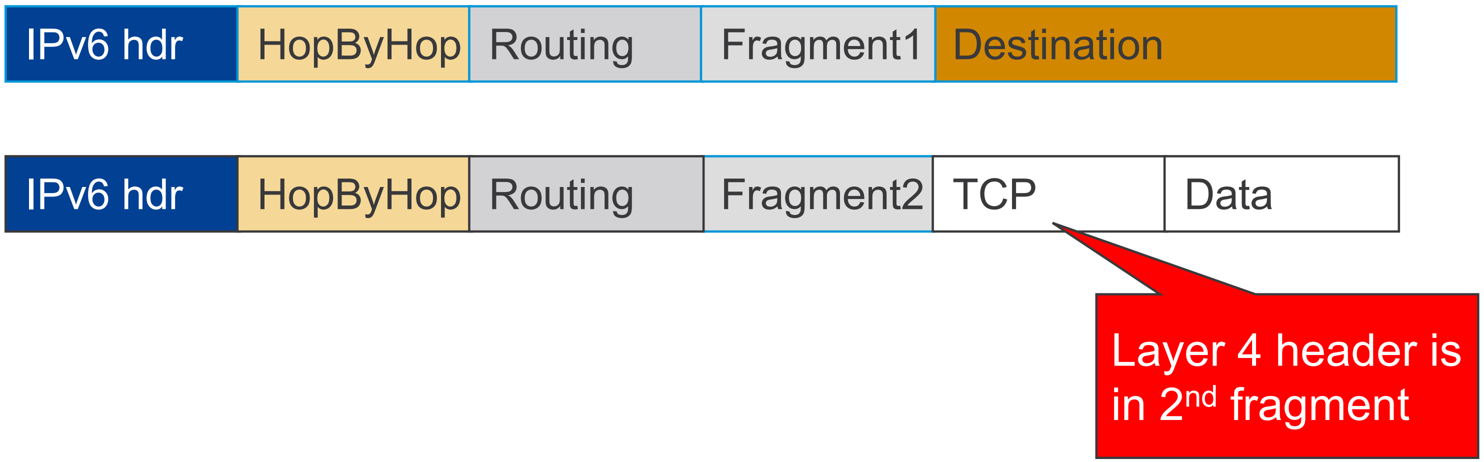
Fragment Header: IPv6

- 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



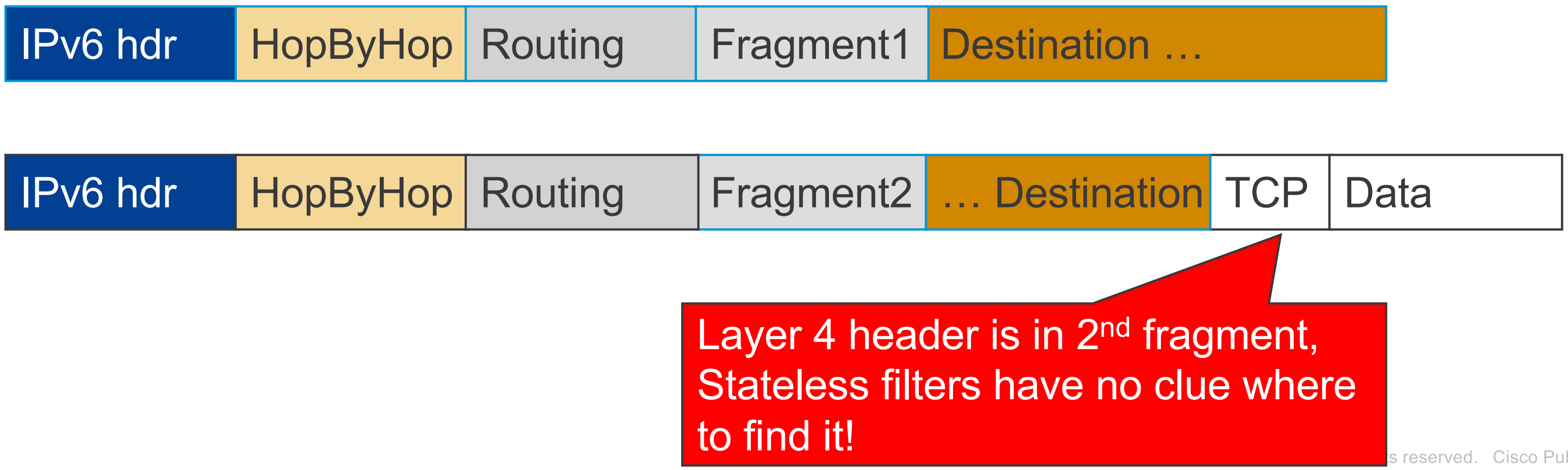
Parsing the Extension Header Chain Fragmentation Matters!

- 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

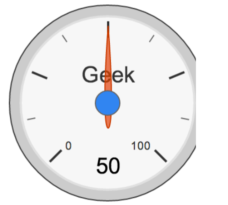
- Layer 4 information could be in 2nd fragment
- But, stateless firewalls could not find it if a previous extension header is fragmented
- RFC 3128 is not applicable to IPv6 but
  - RFC 6980 *'nodes MUST silently ignore NDP ... if packets include a fragmentation header'* ;-)
  - RFC 7112 *'A host that 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)
- Use of **`undetermined-transport`** is strongly recommended
- ASA always drops such initial fragment
- If not supported, consider
  - Bidirectional traffic (TCP, ...): block on the other direction using the source port
  - On an intermediate router: permit TCP, ICMP, UDP, ... Hence blocking everything else (including 1st fragment without layer-4)

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)
- `undetermined-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 ;-)

Extension Header Security Policy

- White list approach for your traffic
  - Only allow the REQUIRED extension headers (and types), for example:
    - Fragmentation header
    - Routing header type 2 & destination option (when using mobile IPv6)
    - IPsec ☺ AH and ESP
    - And layer 4: ICMPv6, UDP, TCP, GRE, ...
  - If your firewall is capable:
    - Drop 1st fragment without layer-4 header
    - Drop routing header type 0
    - Drop/ignore hop-by-hop

Source: Tony Webster, Flickr

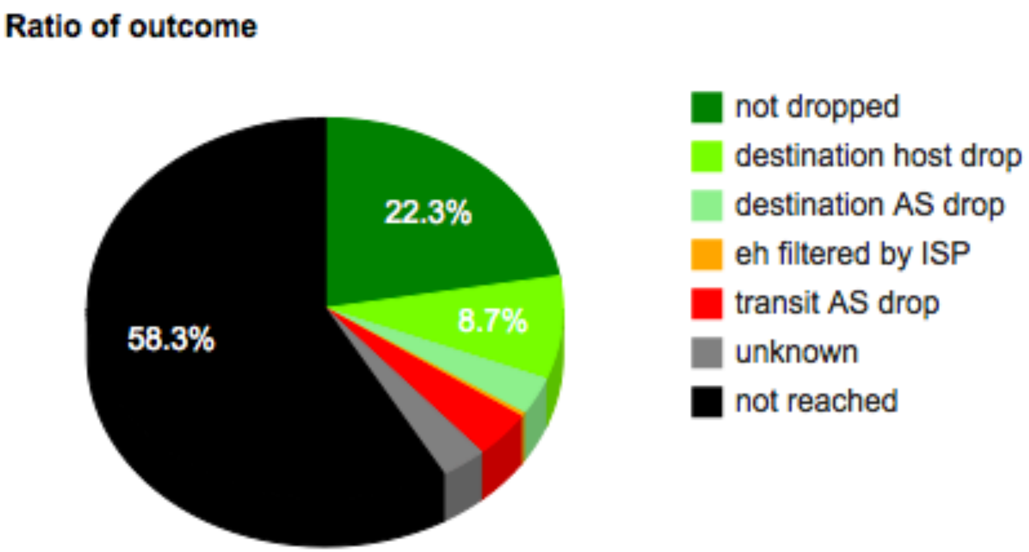
Extension Header Loss over the Internet

- End users SHOULD filter packets with extension headers
- But, what are your ISP and its transit provider doing to your packets?

Source: Paul Townsend, Flickr

- RFC 7872
  - About 20-40% of packets with Ext Hdr are dropped over the Internet

Things Keeps Improving Though



- Current research by Polytechnique Paris (Mehdi Kouhen) and Cisco (Eric Vyncke)
  - And VM provided by Sander Steffann
- http://btv6.vyncke.org/exthdr/index.php?ds=bgp&t=fh (work in progress!)

The Dangerous Mix

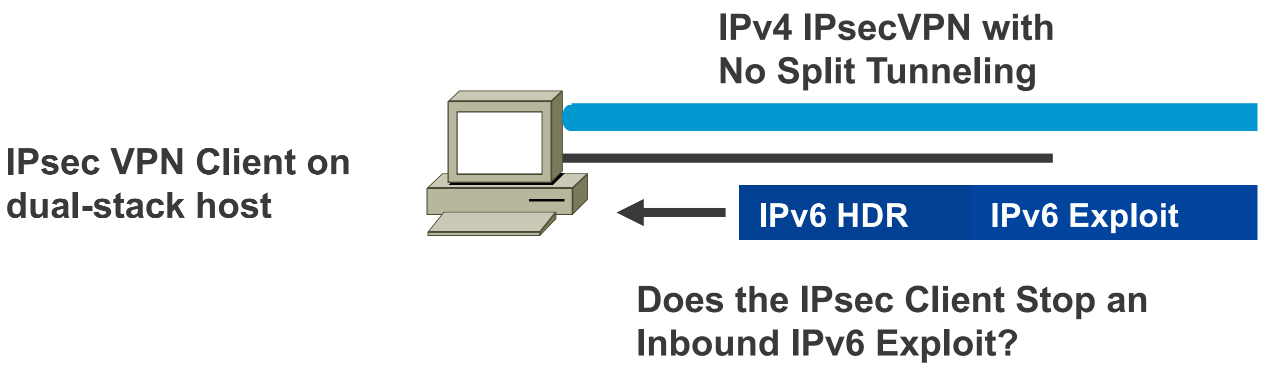
- Atomic fragments (offset = 0, more fragment = 0) are generated when receiving ‘packet-too-big’ for MTU < 1280
  - Being changed with RFC 8021 (informational)
- Non authentication for ICMP ‘packet-too-big’ in most implementation
  - => a third party can force atomic fragmentation
  - => all packets are fragmented
- Sometime fragmentation headers are dropped…

- See http://blog.si6networks.com/2017/01/a-tale-of-bad-decisions-weird-packets.html

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.



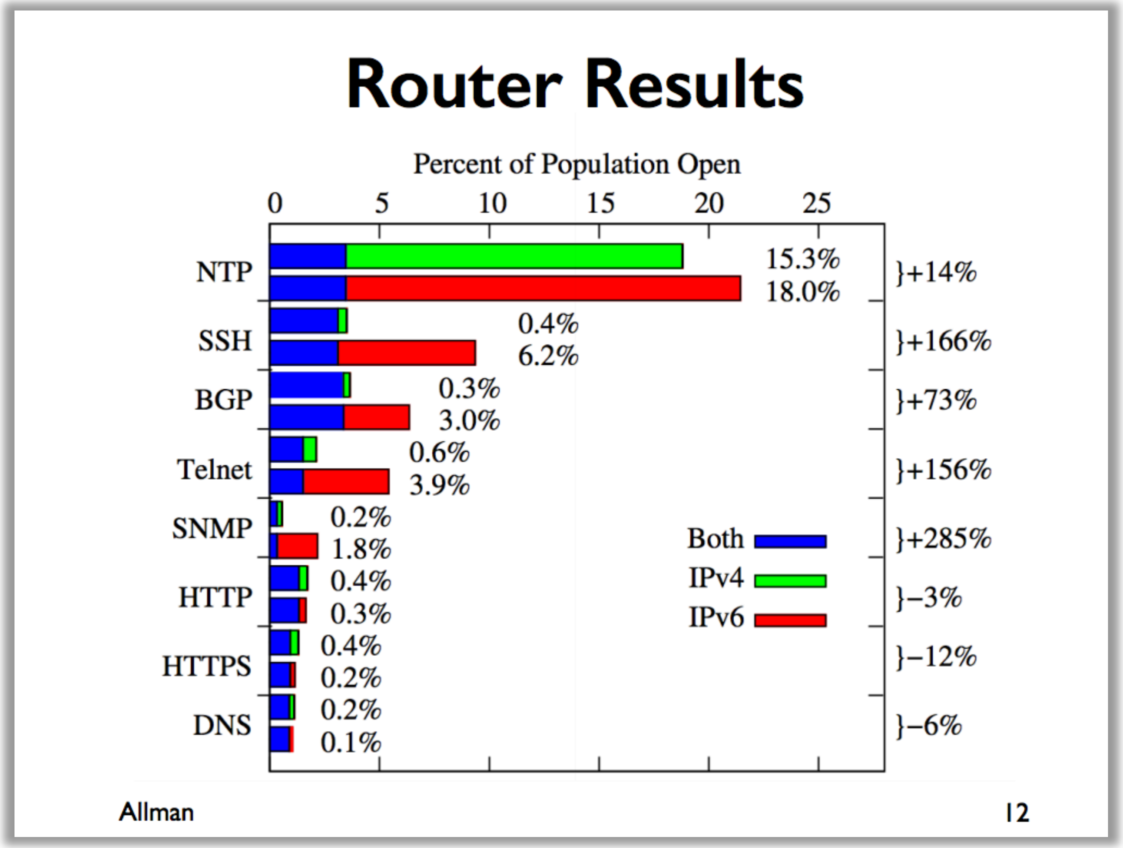
Dual Stack with Enabled IPv6 by Default

- 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

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)

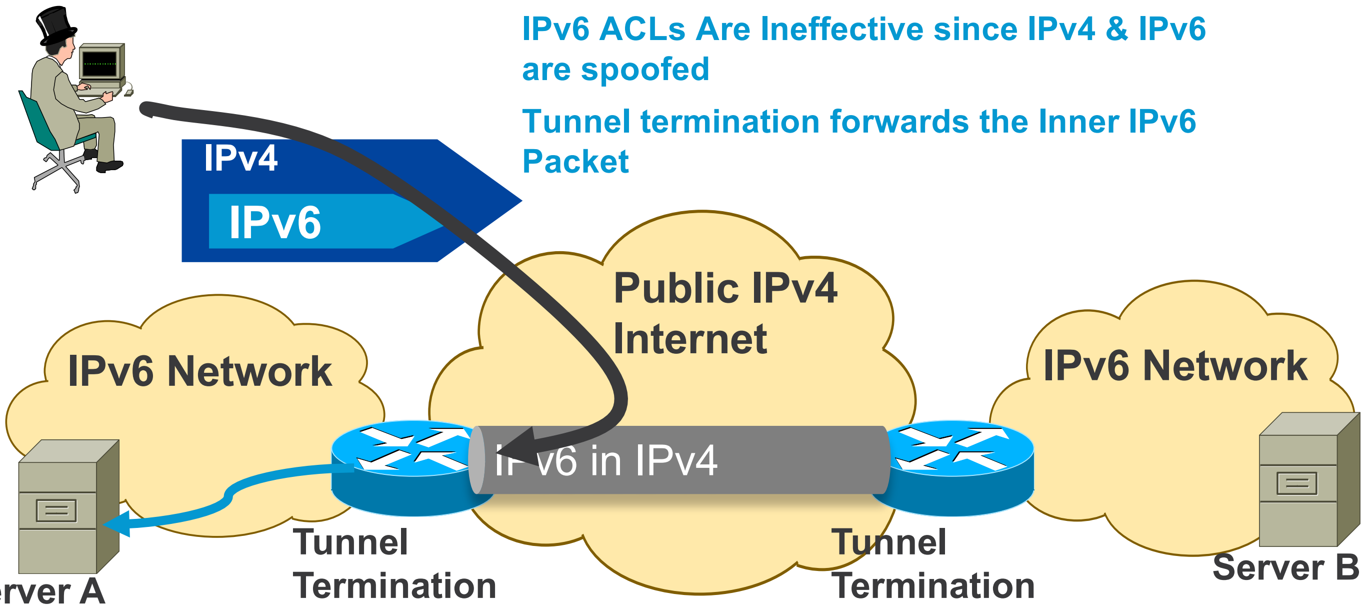
Vulnerability Scanning in a Dual-Stack World

- 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

Specific IPv6 Issue #4
Tunnels

L3-L4 Spoofing in IPv6 When Using IPv6 over IPv4 Tunnels

- Most IPv4/IPv6 transition mechanisms have no authentication built in
- => an IPv4 attacker can inject IPv6 traffic if spoofing on IPv4 and IPv6 addresses



Automatic Tunnels

- These were a real issues with very old Windows (XP & Vista)
- ISATAP: is mainly within an enterprise network, no more used, requires specific configuration
- 6to4 via Internet anycast relay is now historic
- Teredo: never initiated when in an Active Directory domain, default Internet relays are no more available

Can We Block / Detect Rogue Tunnels?

- Using AVC with NBAR2 with ISR G2 Routers
- Using NETFLOW with IPv6 on Routers & Switches

```
IPV6 SRC ADDR                                IPV6 DST ADDR                                TRNS SRC PORT  TRNS DST PORT
st      time last
=============================================  =============================================  =============  =============
==  ============
FE80::20C:29FF:FEEE:B5AB                     FE80::207:7DFF:FE75:5C0                                  0          3481
00  14:42:36.400
2001:DB8:1:10::45                            2001:DB8:1:10::66                                     2048          2048
```

- Using NGIPS

Rule State · Event Filtering · Dynamic State · Alerting · Comments

GID	SID	Message
1	12068	POLICY-OTHER Inbound Teredo traffic detected
1	12066	POLICY-OTHER Inbound Teredo traffic detected
1	12067	POLICY-OTHER Outbound Teredo traffic detected
1	12065	POLICY-OTHER Outbound Teredo traffic detected

- Using NGFW

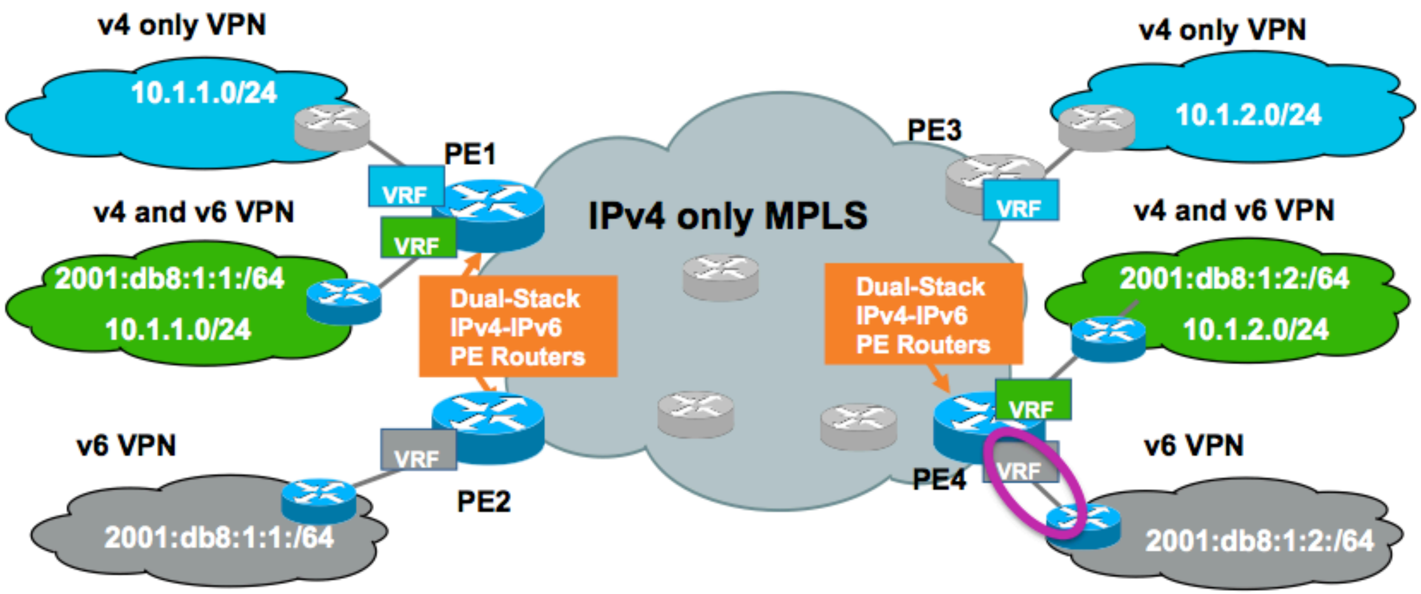
8	Twitter	7	7
9	Microsoft Windows Azure	6	6
10	Teredo IPv6 Tunneled	6	6

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
    - `neighbor FE80::1%Ethernet1/0`
  - Benefit: no remote attack against your infrastructure
  - Implicit infrastructure ACL
  - Note: need to provision loopback for ICMP generation (notably *traceroute* and PMTUD)
  - *See also: RFC7404*
  - LLA can be configured statically (not the EUI-64 default) to avoid changing neighbor statements when changing MAC

SP Transition Mechanism: 6VPE

- 6VPE: the MPLS-VPN extension to also transport IPv6 traffic over a MPLS cloud and IPv4 BGP sessions



6VPE Security

- 6PE (dual stack without VPN) is a simple case
- Security is identical to IPv4 MPLS-VPN, see RFC 4381
- Security depends on correct operation and implementation
  - QoS prevent flooding attack from one VPN to another one
  - PE routers must be secured: AAA, iACL, CoPP …
- MPLS backbones can be more secure than “normal” IP backbones
  - Core not accessible from outside
  - Separate control and data planes
- PE security
  - Advantage: Only PE-CE interfaces accessible from outside
  - Makes security easier than in “normal” networks
  - IPv6 advantage: PE-CE interfaces can use link-local for routing
    - RFC7404 (born draft-ietf-opsec-lla-only)
- => completely unreachable from remote (better than IPv4)

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

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

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

Flexible Flow 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

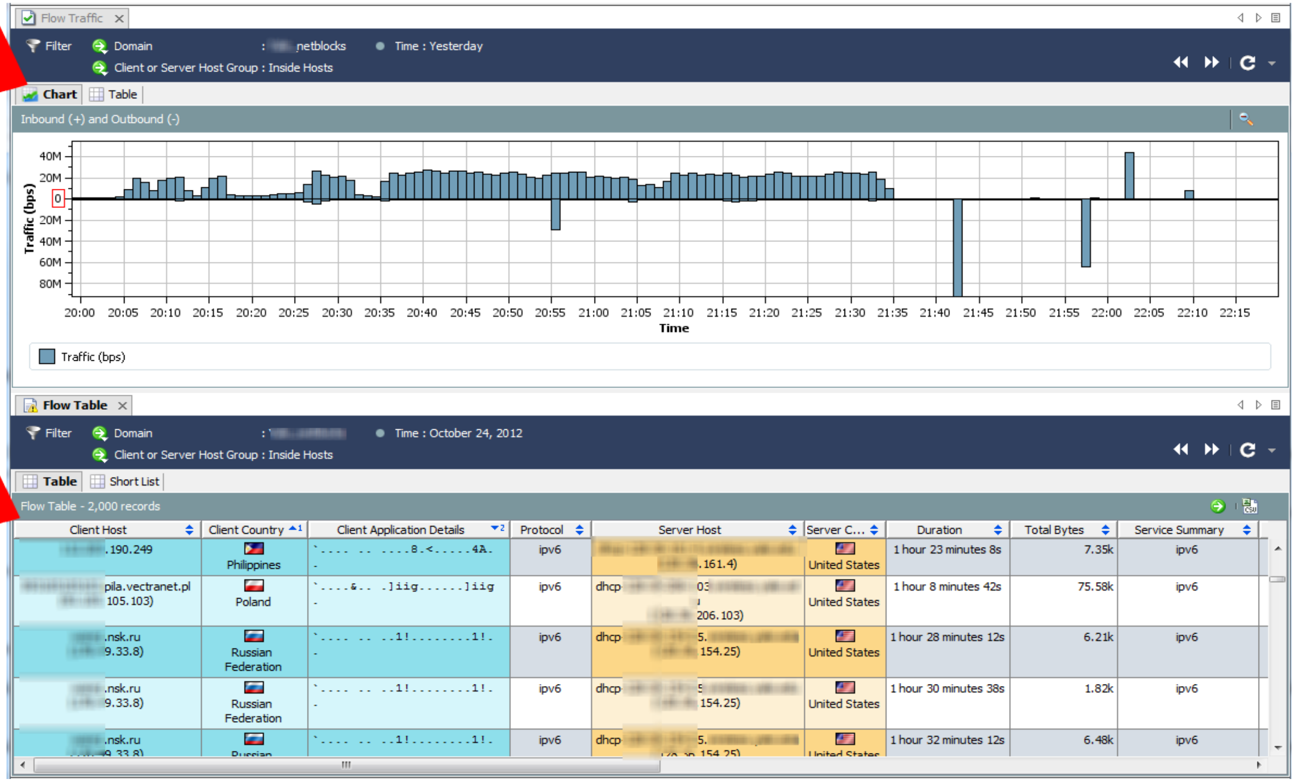
Bits 11-31	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Res	ESP	AH	PAY	DST	HOP	Res	UNK	FRA0	RH	FRA1	Res

- 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

Cisco Threat Defense : Stealth Watch

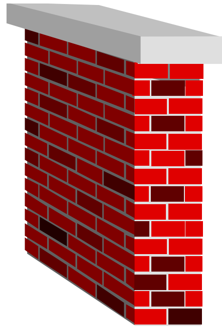
- NetFlow supports IPv6 fields & counters
- Detection & Analysis of IPv6 Traffic to find

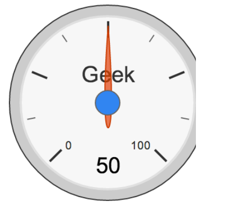
  - unknown IPv6 Routers
  - unknown IPv6 Hosts
  - tunneled traffic
  - malware on Dual Stack Hosts



Enforcing a Security Policy

IOS IPv6 Extended ACL





- Can match on
  - Upper layers: TCP, UDP, SCTP port numbers, ICMPv6 code and type
  - TCP flags SYN, ACK, FIN, PUSH, URG, RST
  - Traffic class (only six bits/8) = DSCP, Flow label (0-0xFFFFF)
- IPv6 extension headers
  - `routing` matches any RH, `routing-type` matches specific RH
  - `mobility` matches any MH, `mobility-type` matches specific MH
  - `dest-option` matches any destination options
  - `auth` matches AH
  - `hbh` matches hop-by-hop (since 15.2(3)T)
- `fragments` keyword matches
  - Non-initial fragments (same as IPv4)
- `undetermined-transport` keyword does not match
  - TCP/UDP/SCTP and ports are in the fragment
  - ICMP and type and code are in the fragment
  - Everything else matches (including OSPFv3…)
  - Only for deny ACE

Check your platform & release as your mileage can vary…

Control Plane Policing for IPv6 Protecting the Router CPU

For Your Reference

- Against DoS with NDP, Hop-by-Hop, Hop Limit Expiration...
- Software routers (ISR, 7200): works with CoPPr (CEF exceptions)

```
policy-map COPPr
 class ICMP6_CLASS
   police 8000
 class OSPF_CLASS
   police 200000
 class class-default
   police 8000
!
control-plane cef-exception
 service-policy input COPPr
```

Cisco Threat Defence: all IPv6 Netflow

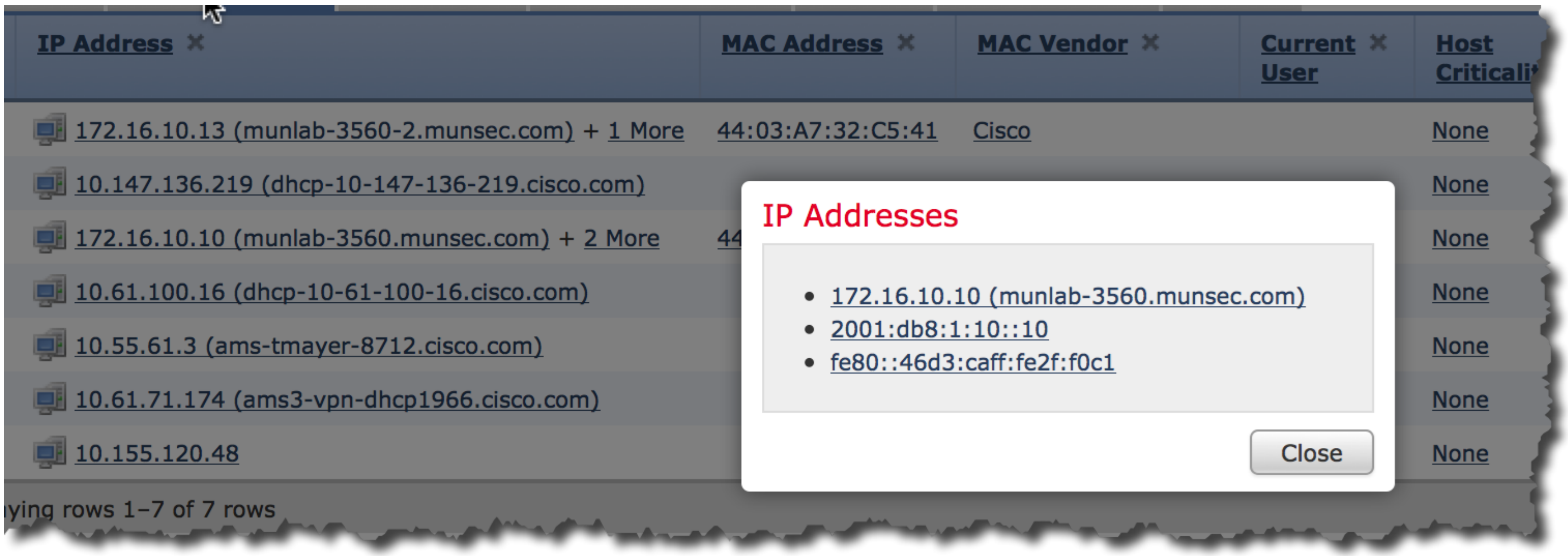
Manage Columns | Filter Results | Export

	START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER BYTES
▶	Dec 18, 2016 3:19:25 AM	0s	2000:1:4:0:204:23ff:fe9e:f16e View URL Data	36110/TCP	Atlanta IPv6	724	HTTP (unclassified)	2.16K	2000:1:2:0:204:23ff:feb4:eb25	80/TCP	Atlanta IPv6	1.45K
▶	Dec 19, 2016 3:19:26 AM	0s	2000:1:4:0:204:23ff:fe9e:f16e View URL Data	36110/TCP	Atlanta IPv6	724	HTTP (unclassified)	2.16K	2000:1:2:0:204:23ff:feb4:eb25	80/TCP	Atlanta IPv6	1.45K
▶	Dec 18, 2016 3:19:25 AM	4m 59s	2000:1:4:0:204:23ff:fe9e:f16e View URL Data	36119/TCP	Atlanta IPv6	224	HTTP (unclassified)	384	2000:1:1:0:213:72ff:fe56:20e9	80/TCP	Atlanta IPv6	160
▶	Dec 19, 2016 3:19:26 AM	4m 58s	2000:1:4:0:204:23ff:fe9e:f16e View URL Data	36119/TCP	Atlanta IPv6	224	HTTP (unclassified)	384	2000:1:1:0:213:72ff:fe56:20e9	80/TCP	Atlanta IPv6	160

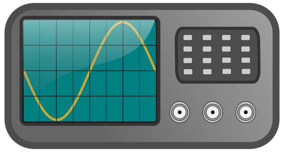
First < 1 > Last

FIREpower NG IPS and IPv6

- FIREsight passive network discovery correlates Events & Host IP
- Very easy to find out the sender / destination in Dual Stacked environments!



Spam over IPv6



- Spammers are also using IPv6 of course...
  - Probably even without knowing it!

Botnet member or open relay from Germany

```
Nov 14 00:44:18 ks postfix/smtpd[22843]: connect from unknown[2a01:4f8:d16:4351::2]
Nov 14 00:44:18 ks postfix/smtpd[22843]: A5CDC155: client=unknown[2a01:4f8:d16:4351::2]
Nov 14 00:44:18 ks postfix/cleanup[22847]: A5CDC155: message-
id=<mw879m.1ci1jl@front.chemise-homme234.com>
Nov 14 00:44:18 ks postfix/qmgr[3578]: A5CDC155: from=<bck@chemise-homme234.com>,
size=27742, nrcpt=1 (queue active)
```

- So, we need to fight IPv6 spam!
  - Content filtering: nothing has changed
  - Sender authentication (DKIM, SPF, DMARC) works with IPv6
  - Sender reputation works with Cisco Senderbase

Summary of Cisco IPv6 Security Products

- ASA Firewall (Since version 7.0 released 2005)
  - Extension header filtering and inspection (ASA 8.4.2)
  - Dual-stack ACL & object grouping (ASA 9.0)
- Email Security Appliance (ESA) IPv6 support since 7.6.1 (May 2012)
- Web Security Appliance (WSA) with explicit and transparent proxy
- FIREpower NGIPS provides Decoder for IPv4 & IPv6 Packets
- Cisco Threat Defense / StealthWatch: mostly forever including SMC

- FirePOWER Threat Defence (FTD) no IPv6 inspection support on the GUI
- FirePOWER Device Manager (FDM) no IPv6 support
- Cisco Cloud Web Security (ScanSafe) no IPv6
- Cisco Umbrella, answers AAAA but cannot manage policy for IPv6 network
- ISE does not support IPv6 (no IPv6 ACL, no IPv6 transport)

Meraki growing IPv6 Support

Secure IPv6 over IPv4/6 Public Internet

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

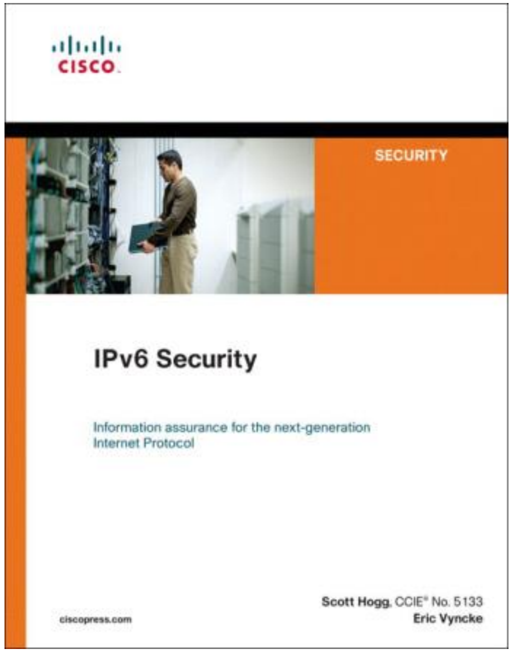
Public Network	Site 2 Site	Remote Access
IPv4	▪ 6in4/GRE Tunnels Protected by IPsec ▪ DMVPN 12.4(20)T ▪ FlexVPN	▪ ISATAP Protected by RA IPsec ▪ SSL VPN Client AnyConnect
IPv6	▪ IPsec VTI 12.4(6)T ▪ DMVPN 15.2(1)T ▪ FlexVPN	▪ SSL VPN Client AnyConnect 3.1 & ASA 9.0

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)

CISCO