CyberExcellence
By CyberWal

CISCO™

2023::3/6
Is IPv6 more Secure than IPv4?

Eric Vyncke, Distinguished Engineer, Cisco Belgium
Co-author of RFC 9099

A Quick Refresh...

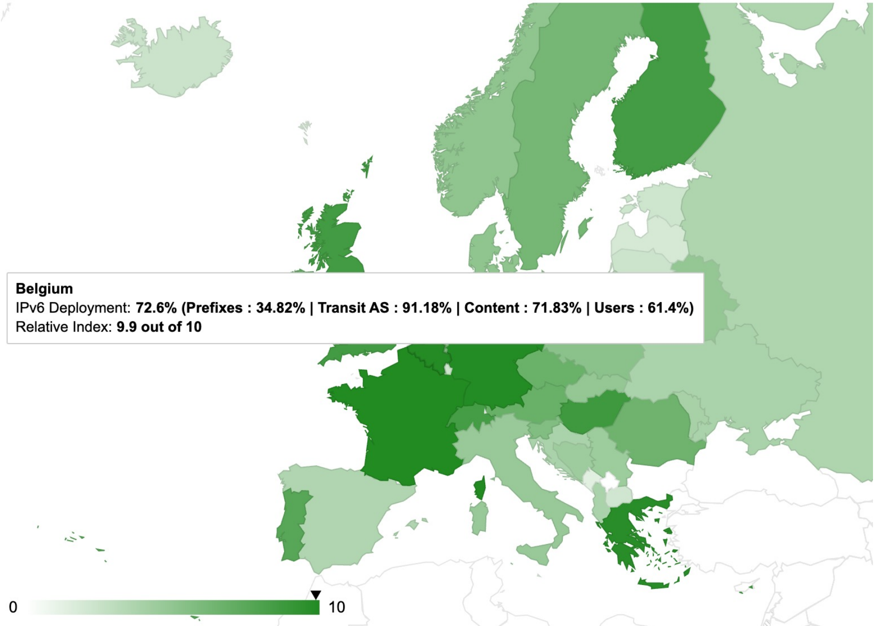
IPv6 in One Slide

- IPv6 is IPv4 with larger addresses
  - 128 bits vs. 32 bits
- Data-link layer unchanged: Ethernet, xDSL, …
- Transport layer unchanged: UDP, TCP, …
- Enabled in all hosts OS for 10+ years

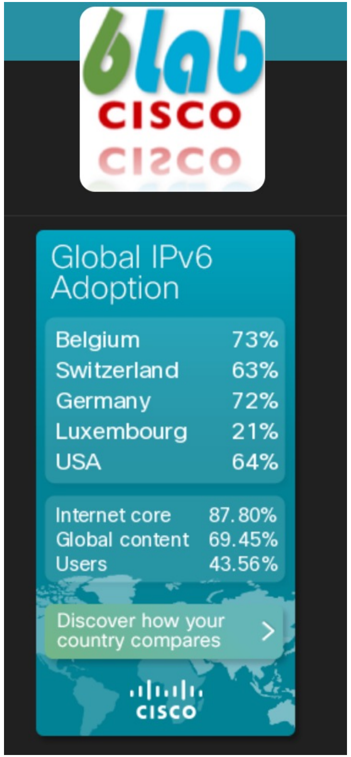
Address Representation

- Format:
  - x:x:x:x:x:x:x:x where x is 16 bits hexadecimal field
    - 2001:0000:130f:0000:0000:09c0:876a:130b
    - Case insensitive (lower case preferred)
  - Leading zeros in a field are optional:
    - 2001:0:130f:0:0:9c0:876a:130b
  - Successive fields of 0 are represented as ::, but only once in an address:
    - 2001:0:130f::9c0:876a:130b
    - ~~2001::130f::9c0:876a:130b~~
    - ff02:0:0:0:0:0:0:1 => ff02::1
    - 0:0:0:0:0:0:0:1 => ::1
    - 0:0:0:0:0:0:0:0 => ::

Where are we ?



Belgium
IPv6 Deployment: **72.6% (Prefixes : 34.82% | Transit AS : 91.18% | Content : 71.83% | Users : 61.4%)**
Relative Index: **9.9 out of 10**



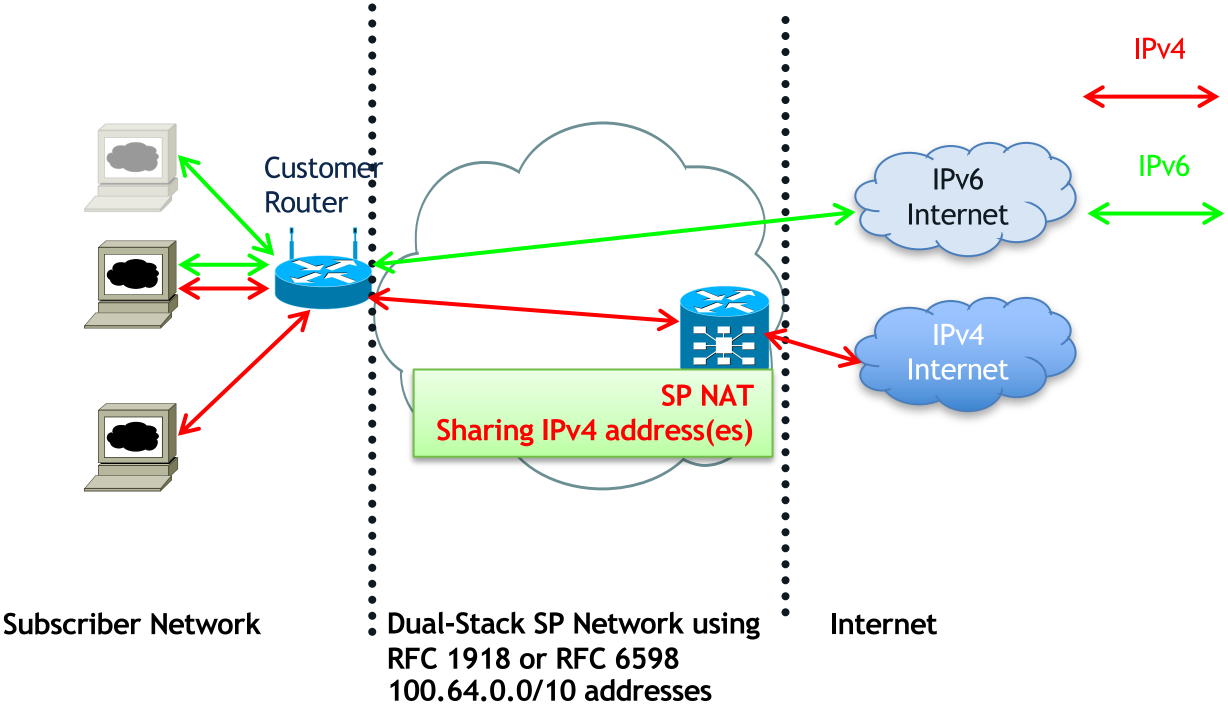
Global IPv6 Adoption

Belgium	73%
Switzerland	63%
Germany	72%
Luxembourg	21%
USA	64%

Internet core	87.80%
Global content	69.45%
Users	43.56%

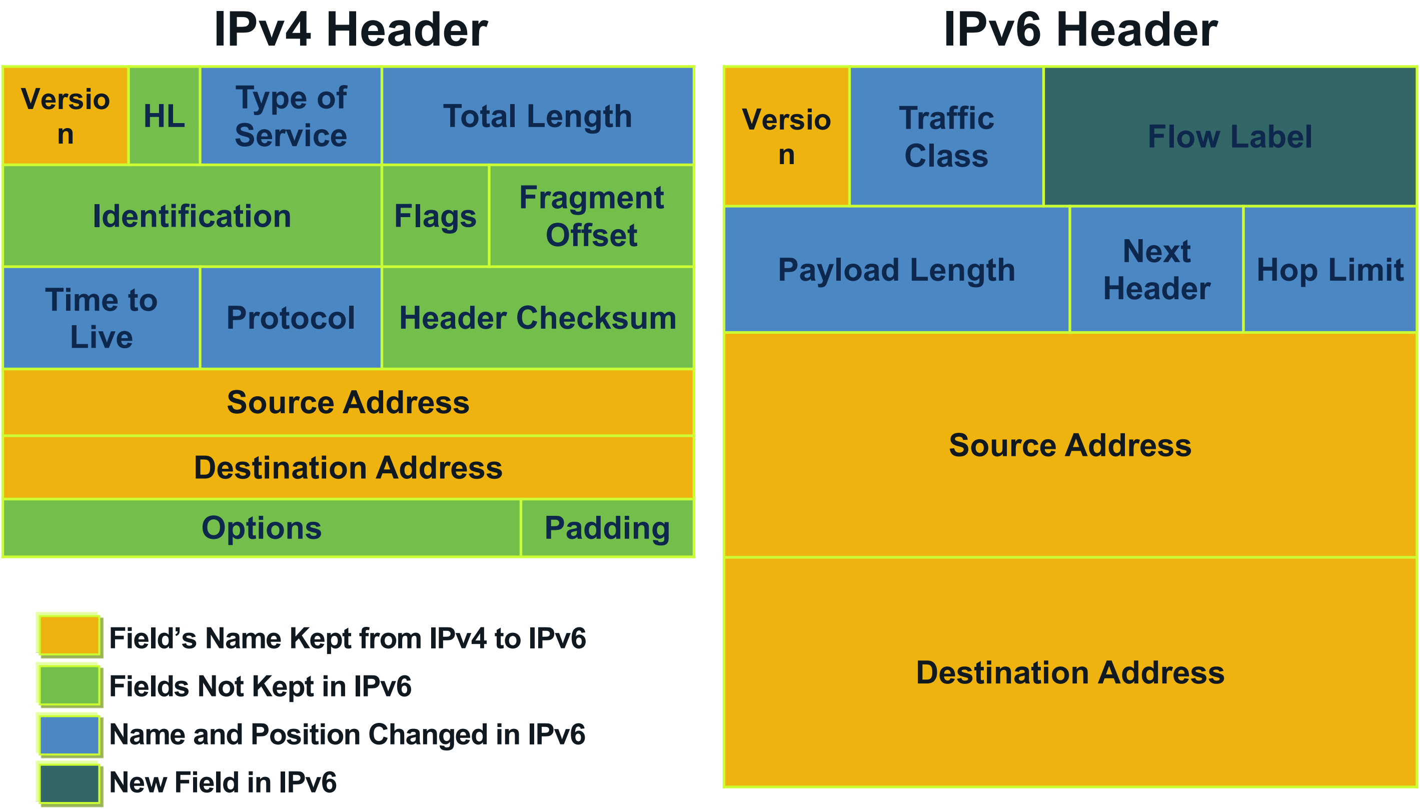
Source: https://6lab.cisco.com

Without IPv6: Dual-Stack with SP Double NAT



IPv4 vs. IPv6 Header Comparison

IPv4 and IPv6 Header Comparison



IPv4 Header

Versio n | HL | Type of Service | Total Length

Identification | Flags | Fragment Offset

Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options | Padding

IPv6 Header

Versio n | Traffic Class | Flow Label

Payload Length | Next Header | Hop Limit

Source Address

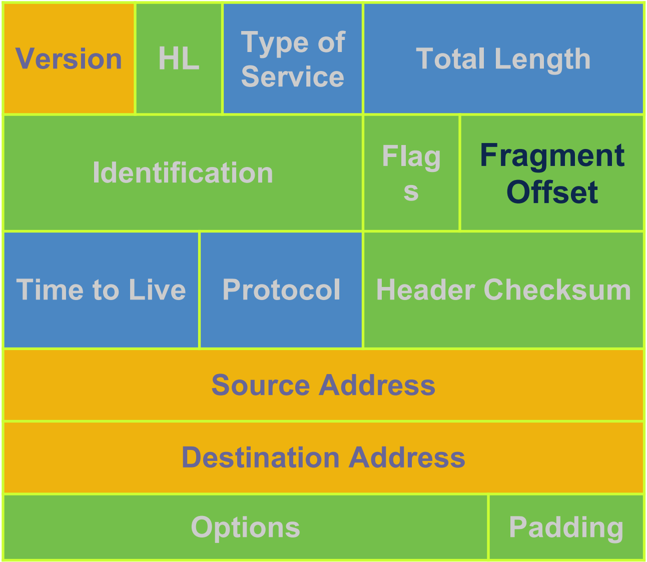
Destination Address

- 🟨 Field’s Name Kept from IPv4 to IPv6
- 🟩 Fields Not Kept in IPv6
- 🟦 Name and Position Changed in IPv6
- ⬛ New Field in IPv6

IPv4 and IPv6 Header Comparison Fields Removed

- Fragmentation: IPv6 does not do fragmentation
- If a sending host wants to do fragmentation, it will do it through extension headers

IPv4 Header

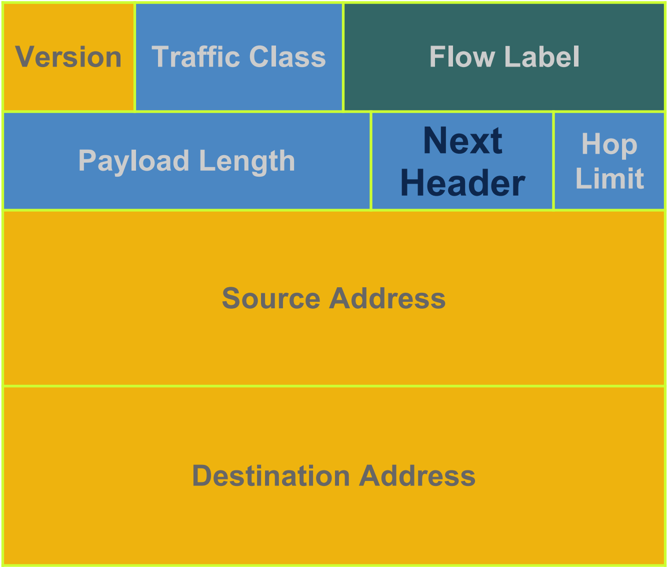


Version	HL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding

IPv4 and IPv6 Header Comparison
Fields Renamed

- Next header: similar to the protocol field in IPv4
- The value in this field tells you what type of information follows
  - E.g., TCP, UDP, extension header

IPv6 Header



Version

Traffic Class

Flow Label

Payload Length

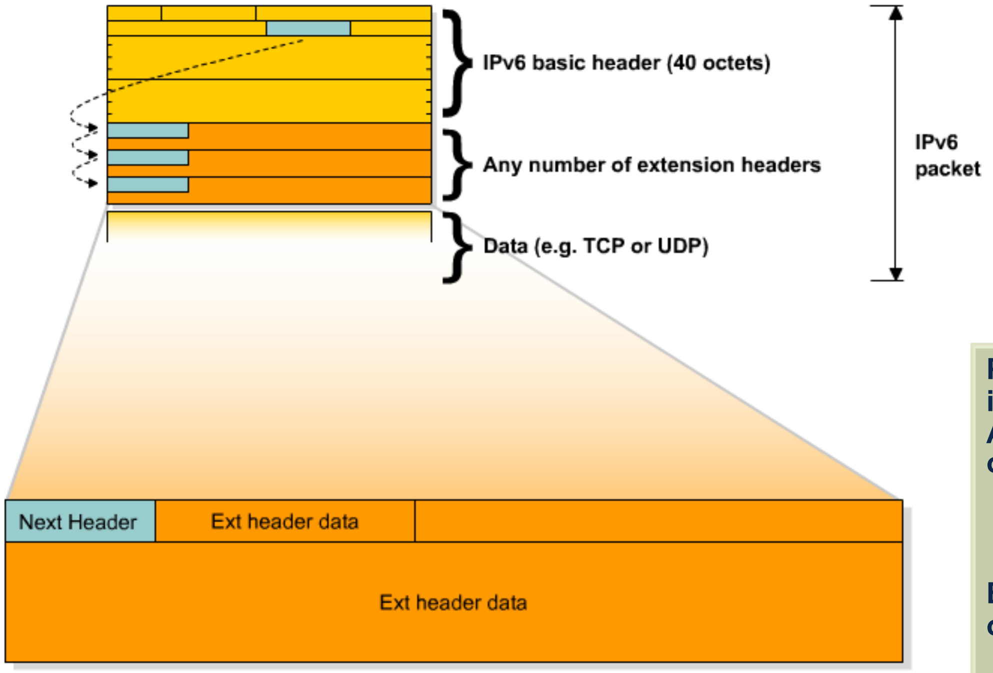
Next Header

Hop Limit

Source Address

Destination Address

Extension Headers (RFC8200)



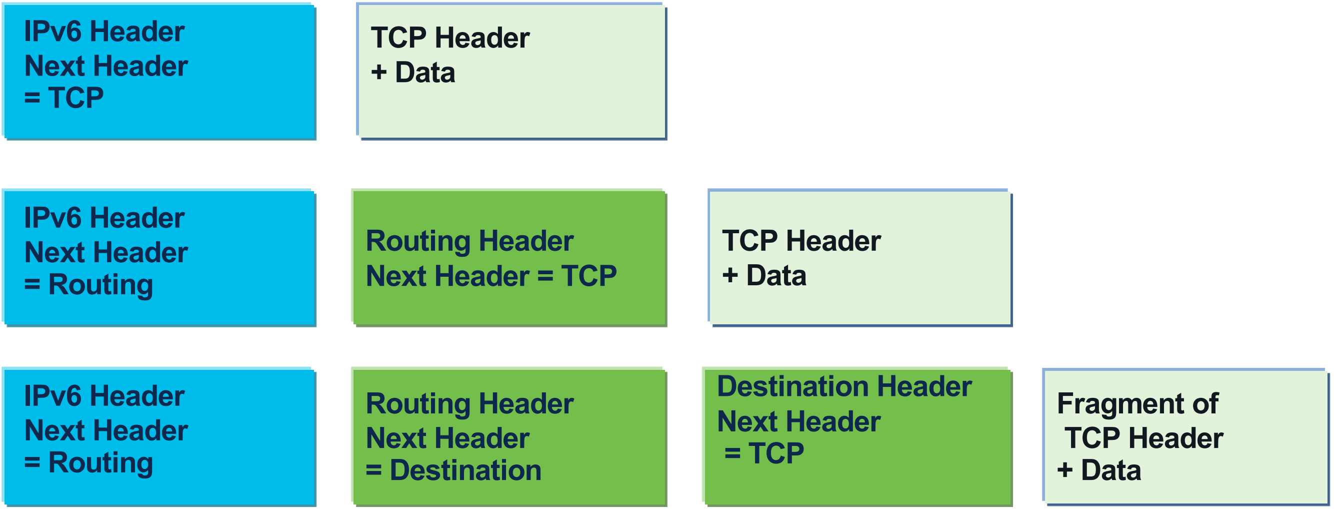
Processed only by node identified in IPv6 Destination Address field => much lower overhead than IPv4 options

- exception: Hop-by-Hop Options header

Eliminated IPv4's 40-octet limit on options

- In IPv6, limit is total packet size, or Path MTU in some cases

Extension Headers



IPv6 Header
Next Header
= TCP

TCP Header
+ Data

IPv6 Header
Next Header
= Routing

Routing Header
Next Header = TCP

TCP Header
+ Data

IPv6 Header
Next Header
= Routing

Routing Header
Next Header
= Destination

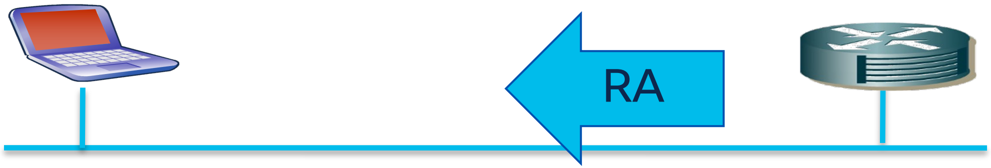
Destination Header
Next Header
= TCP

Fragment of
TCP Header
+ Data

Router Advertisment Provisioning StateLess Address Auto-Configuration (SLAAC)

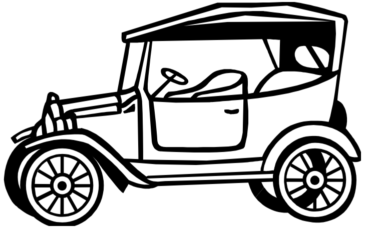
- M-Flag – Stateful DHCPv6 to acquire IPv6 address
- O-Flag – Stateless DHCPv6 in addition to SLAAC
- Preference Bits – Low, Med, High
- Options – Prefix Information, Length, Flags
  - L bit – Only way a host get a On Link Prefix
  - A bit – Set to 0 for DHCP to work properly

```
Type: 134 (RA)
Code: 0
Checksum: 0xff78 [correct]
Cur hop limit: 64
∞ Flags: 0x84
    1... .... = Managed (M flag)
    .0.. .... = Not other (O flag)
    ..0. .... = Not Home (H flag)
    ...0 1... = Router pref: High
Router lifetime: (s)1800
Reachable time: (ms) 3600000
Retrans timer: (ms) 1000
ICMPv6 Option 3 (Prefix Info)
Prefix length: 64
∞ Flags: 0x80
    1... .... = On link (L Bit)
    .1.. .... = No Auto (A Bit)
Prefix: 2001:0db8:4646:1234::/64
```



IPv6 Security Myths...

IPv6 Myths: Better, Faster, More Secure



Sometimes, newer means better and more secure

Sometimes, experience IS better and safer!

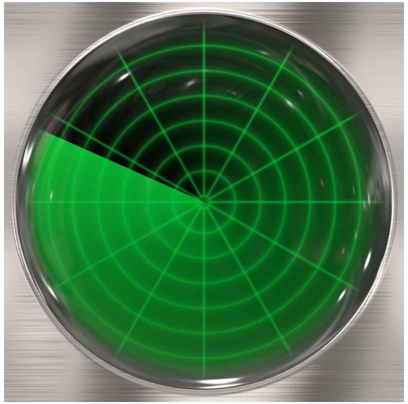
Source: Microsoft clip-art gallery

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

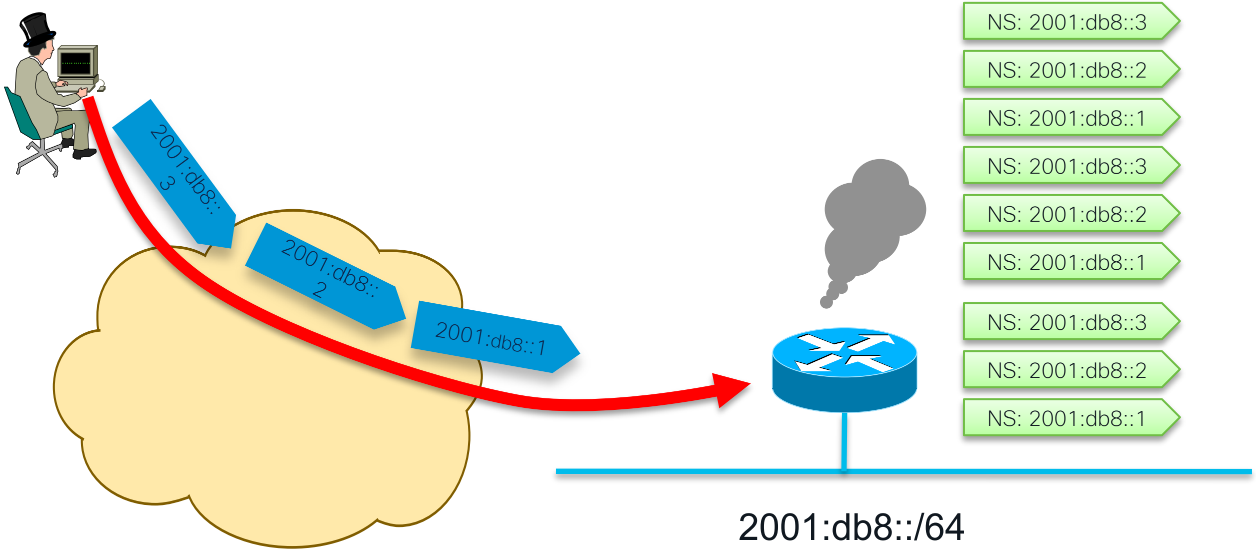
- If using EUI-64 addresses, just scan 2^{48}
  - Or even 2^{24} if vendor OUI is known...
- Public servers will still need to be DNS reachable
  - More information collected by Google...
- Increased deployment/reliance on dynamic DNS
  - More information will be in DNS
- Using peer-to-peer clients gives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

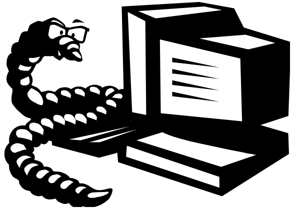
Potential router CPU/memory attacks if aggressive scanning

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

Local router DoS with NS/RS/...



Viruses and Worms in IPv6



- Viruses and IM/email 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

- “IPv6 mandates the implementation of IPsec”
- Some organizations believe that IPsec should be used to secure all flows…

> ***“Security expert, W., a professor at the University of <foo> in the UK, told <newspaper> the new protocol system – IPv6 – comes with a security code known as IPSEC that would do away with anonymity on the web.***
>
> ***If enacted globally, this would make it easier to catch cyber criminals, Prof W. said.”***

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

- IPv6 originally mandated the implementation of IPsec (but not its use)
- Now, RFC 8504 "**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 ?

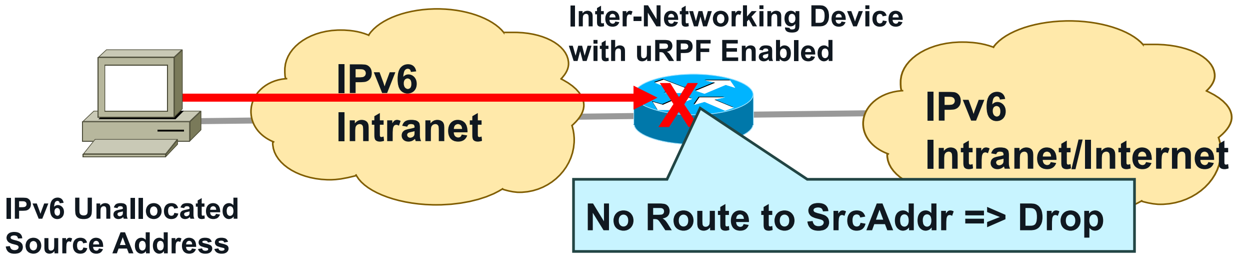
Recommendation: do not use IPsec end to end within an administrative domain.

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

Security Issues Shared by IPv6 and IPv4

IPv6 Bogon and Anti-Spoofing Filtering

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


IPv6 Unallocated Source Address
IPv6 Intranet
Inter-Networking Device with uRPF Enabled
IPv6 Intranet/Internet
No Route to SrcAddr => Drop

ICMPv4 vs. ICMPv6

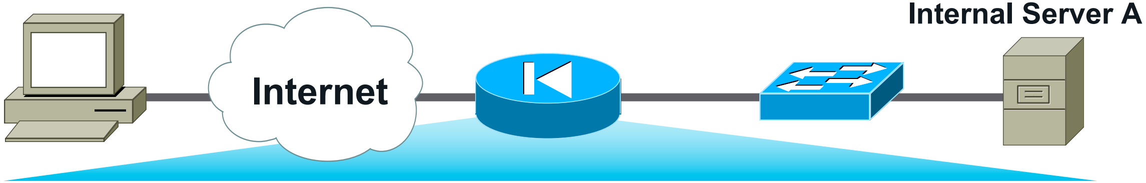
- Significant changes
- More relied upon

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

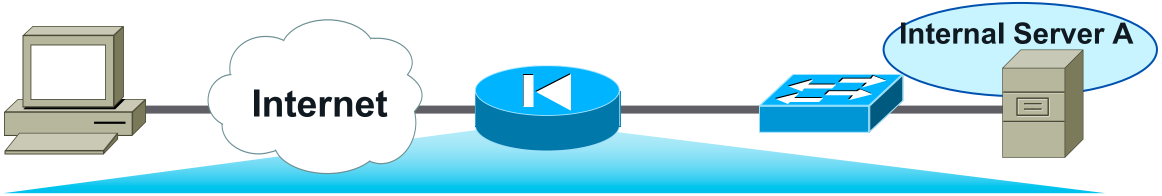
Border Firewall Policy



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

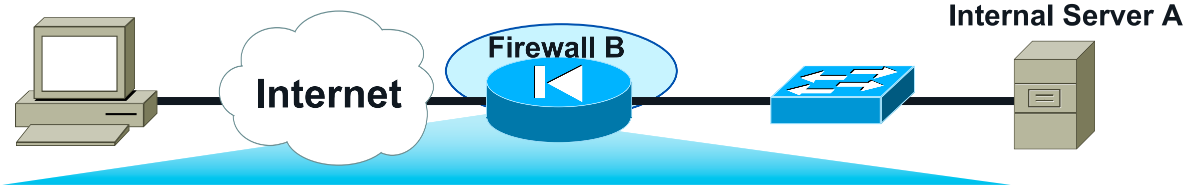
RFC 4890: Border Firewall Transit Policy



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

Potential Additional ICMPv6

RFC 4890: Border Firewall Transit Policy

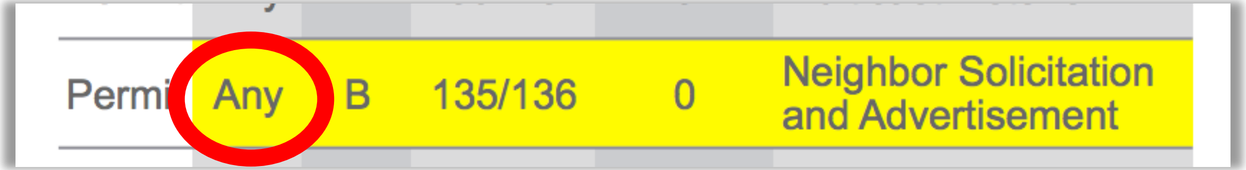


Action	Src	Dst	ICMPv6 Type	ICMPv6 Code	Name
Permit	Any	B	2	0	Packet too Big
Permit	Any	B	4	0	Parameter Problem
Permit	Any	B	130–132	0	Multicast Listener
Permit	Any	B	135/136	0	Neighbor Solicitation and Advertisement
Deny	Any	Any			

For locally generated by the device

Remote NDP Floods...

- Hot from the press https://blog.apnic.net/2023/01/30/interesting-ipv6-ndp-observation/ (Feb 2023)
- 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"

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

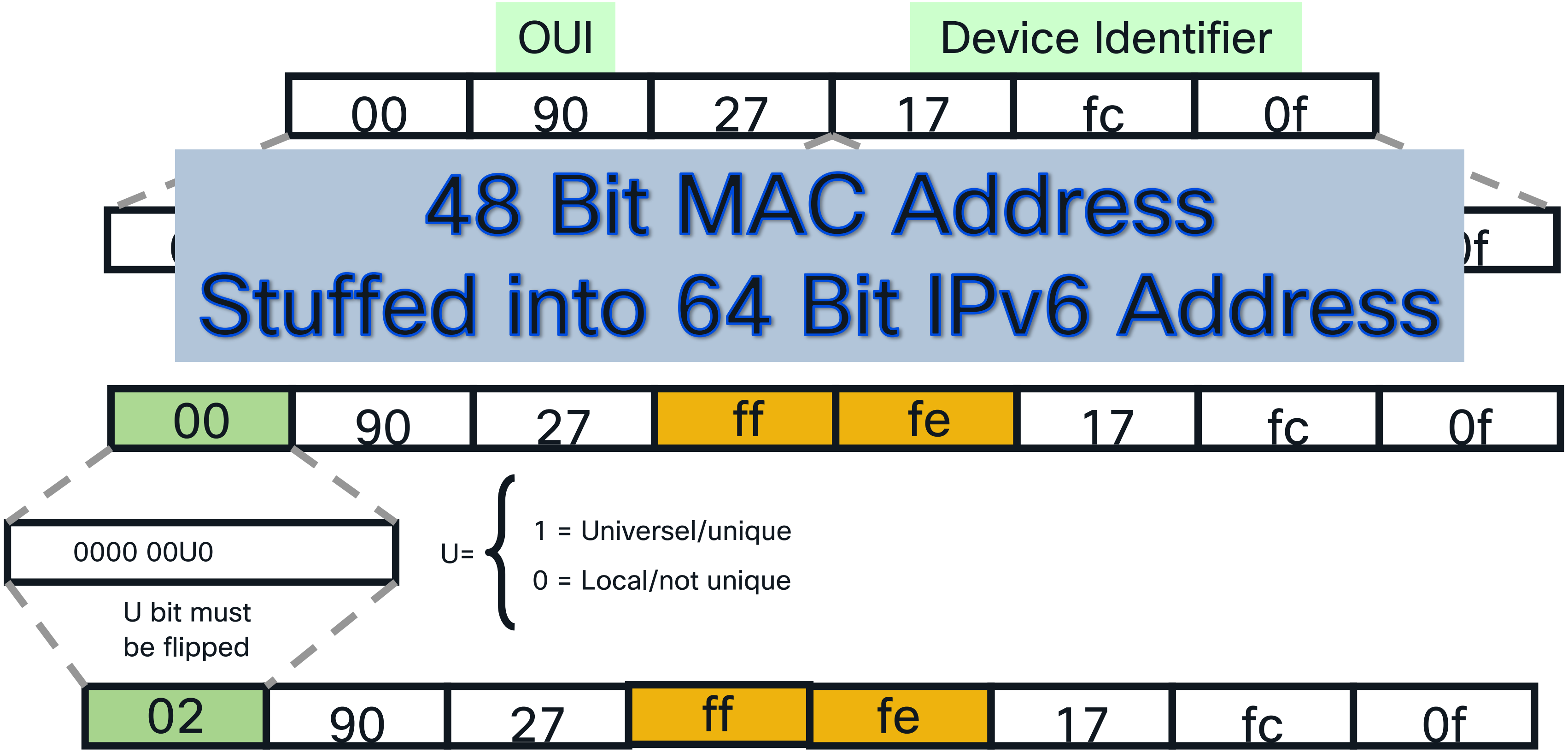
IPv6 Attacks with Strong IPv4 Similarities

Good news
IPv4 IPS
signatures can be
re-used

- 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

Security Issues Specific to IPv6

Extended Unique Identifier (EUI64)



00	90	27	17	fc	0f

48 Bit MAC Address
Stuffed into 64 Bit IPv6 Address

00	90	27	ff	fe	17	fc	0f

0000 00U0

U bit must
be flipped

U= 1 = Universel/unique
0 = Local/not unique

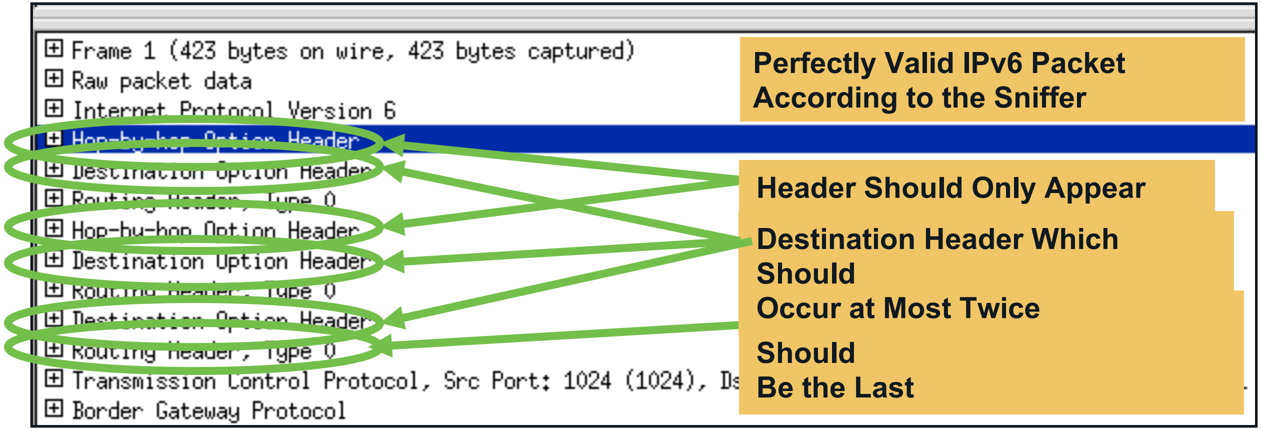
02	90	27	ff	fe	17	fc	0f

RFC 8941 Temporary Addresses Extensions

- Temporary addresses for IPv6 host client applications:
  - Inhibit device/user tracking when EUI-64 was used
  - Random 64-bit interface ID per IPv6 prefix
    - then run Duplicate Address Detection before using it
  - Rate of change based on local policy (typical once per day)
- Enabled by default in Windows, Android, iOS, Mac OS/X ...
- Excellent for privacy
- Makes operation more complex:
  - Cannot have a client specific static ACL
  - User attribution more complex (without RFC 7217 – stable privacy address)

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 which can filter on headers



```
⊞ Frame 1 (423 bytes on wire, 423 bytes captured)
⊞ Raw packet data
⊞ Internet Protocol Version 6
⊞ Hop-by-hop Option Header
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Hop-by-hop Option Header
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Destination Option Header
⊞ Routing Header, Type 0
⊞ Transmission Control Protocol, Src Port: 1024 (1024), Ds
⊞ Border Gateway Protocol
```

Perfectly Valid IPv6 Packet According to the Sniffer

Header Should Only Appear

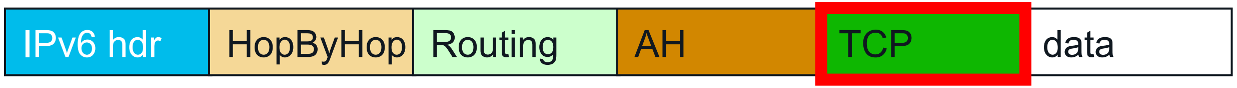
Destination Header Which Should Occur at Most Twice

Should Be the Last

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

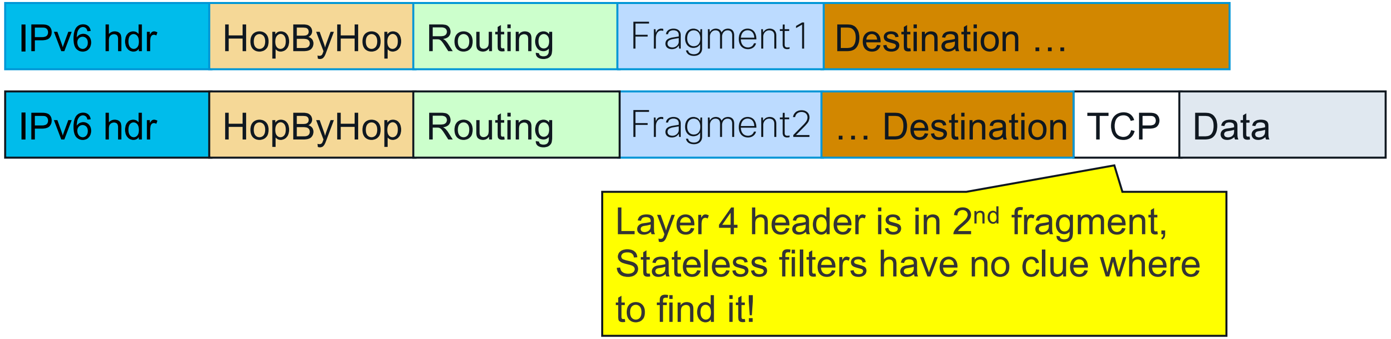


Fragment Header: IPv6

- In IPv6 fragmentation is done only by the end system
  - Tunnel end-points are end systems => Fragmentation / re-assembly can happen inside the network
- RFC 5722/RFC 8200: overlapping fragments => MUST drop the packet. Most OS implement it since 2012
- Attackers can still fragment in intermediate systems on purpose ==> a great obfuscation tool

Parsing the Extension Header Chain

- Layer-4 information could be in 2nd fragment
- But stateless firewalls could not find it if a previous extension header is fragmented



Layer 4 header is in 2nd fragment, Stateless filters have no clue where to find it!

RFC 8200: “If the first fragment does not include all headers through an Upper-Layer header, then that fragment should be discarded”

Drop those fragments, if possible, at the edge:

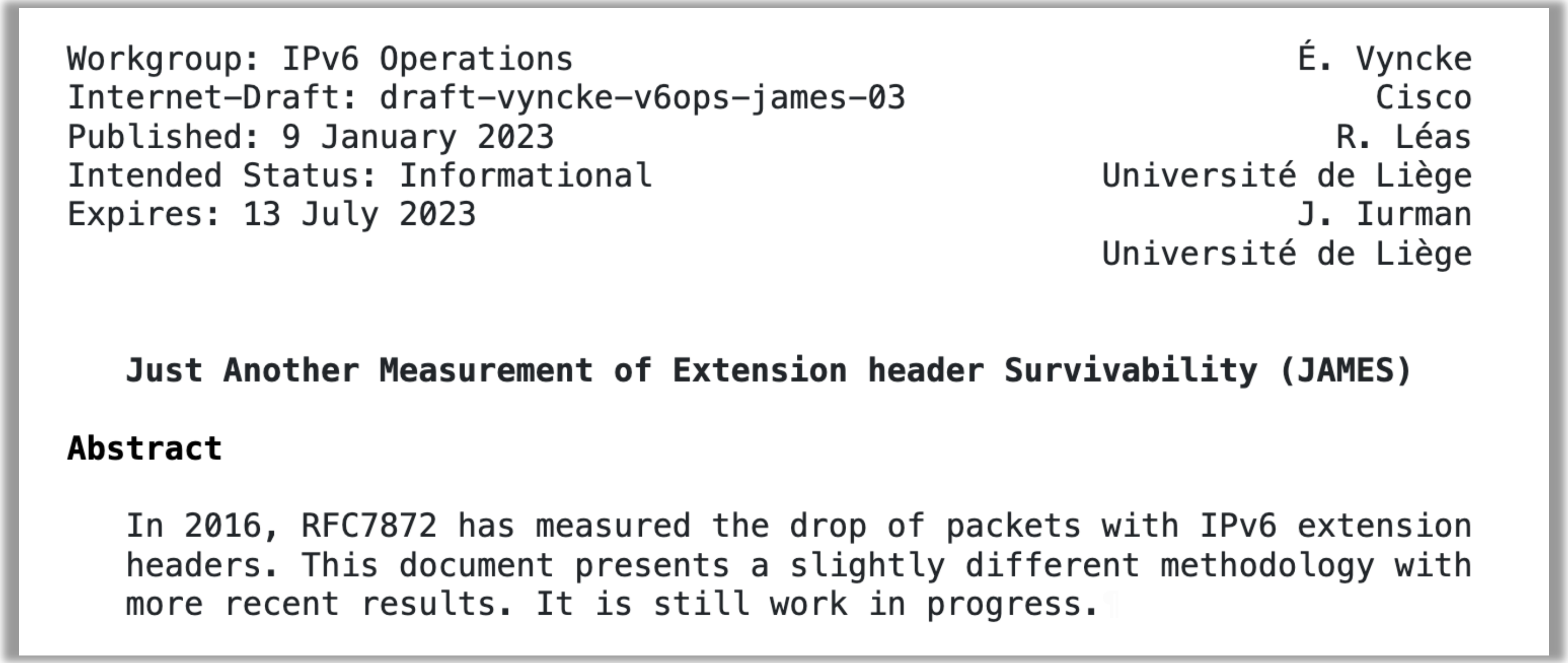
- With a firewall
- With IOS ACL: `deny ipv6 any any undetermined-transport`

Extension Header Security Policy

- Permit list approach for your traffic
- Only allow the LOCALLY-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 next-headers/transports: ICMPv6, UDP, TCP, GRE, OSPF, ...
- If your router/firewall is capable, then drop packets with:
  - 1st fragment without layer-4 header
  - Out-of-order extension headers
  - routing header type 0
  - hop-by-hop (drop or ignore)
  - Filter routing header type 4 (SRv6) at your **edge** if you use it
- See also RFC 9288

Source: Tony Webster, Flickr

draft-vyncke-v6ops-james



Workgroup: IPv6 Operations
Internet-Draft: draft-vyncke-v6ops-james-03
Published: 9 January 2023
Intended Status: Informational
Expires: 13 July 2023

É. Vyncke
Cisco
R. Léas
Université de Liège
J. Iurman
Université de Liège

Just Another Measurement of Extension header Survivability (JAMES)

Abstract

In 2016, RFC7872 has measured the drop of packets with IPv6 extension headers. This document presents a slightly different methodology with more recent results. It is still work in progress.¶

NDP ≠ ARP

- NDP cache could contain up to 2^{64} entries per interface
  - Need to protect the cache to prevent DoS (local/remote)
  - Rate limiting + size limit (default in most OS)
- NDP is as “secure” as ARP…
  - No authentication, NDP messages can be spoofed
- IPv6 does not need DHCPv6 with StateLess Address AutoConfiguraton (SLAAC)
  - Not centralized/trustable source of truth for IPv6 addresses

Source: Library of Congress

Security the Link-Layer

- The abandoned crypto way: SEND (SEcure Neighbor Discovery)
- Point-to-point links:
  - LLA-only or a /127 to prevent NDP cache exhaustion attack
- Broadcast media:
  - First hop security: RA guard, DHCP guard, source guard, device tracking, ...
  - Snoop DHCPv6 (if available) and NDP (but stateless) to build a device-tracking table
  - Drop packets whose <IP, MAC, port> violate the device-tracking table

  - This table will be useful also for *monitoring/auditing*

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

- Network Prefix Translation, RFC 6296,
- 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

NAT does not Protect IoT

“Early 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with Mirai bot code was discovered. The number of IoT devices which were previously safely hidden inside corporate perimeters, vastly exceeds those directly accessible from the Internet, allowing for the creation of botnets with unprecedented reach and scale.”

“The call is coming from inside the house! Are you ready for the next evolution in DDoS attacks?”

Steinthor Bjanarson, Arbor Networks, DEFCON 25

PCI DSS 3.0 Compliance and IPv6

- Payment Card Industry Data Security Standard *(since 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

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 <u>not</u> 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

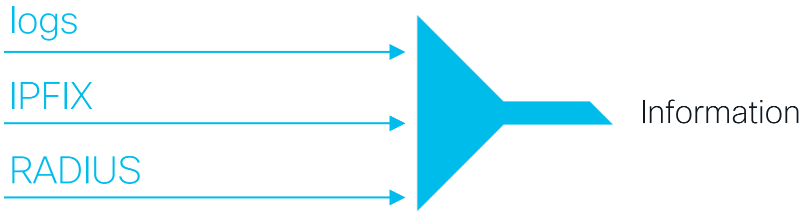
- Finding all hosts:
  - Address enumeration does not work for IPv6
  - Need to rely on DNS or NDP caches or NetFlow
- Vulnerability scanning
  - IPv4 global address, IPv6 global address(es) (if any), IPv6 link-local address
  - Some services are single stack only (currently mostly IPv4 but who knows...)
  - 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

Logging & Monitoring

Multiple Facets to IPv6 Addresses

- Every host can have multiple IPv6 addresses simultaneously
  - Need to do correlation!
  - Alas, few 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…

Information Sources



- Log files, beware: the same IPv6 address can be written in different ways
  - Try to use the canonical format, RFC 5952: 2001:db8::bad
- IPFIX (Netflow v9), NETCONF/SNMP for live information (esp. NDP cache for *<IP, MAC>* bindings)
- RADIUS accounting is useful for *<IP, MAC,* ***username****>* bindings
- DHCPv6 leases do not include client MAC addresses and not always used

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

```
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?

- 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…

- Not so attractive ☹
- Only supported in Windows Vista, and Windows 7, Max OS/X Lion, iOS
  - Not in Linux (default installation), Android, …
- Windows 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

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…

Security Takeaway

- So, nothing really new in IPv6
  - Reconnaissance: address enumeration replaced by DNS enumeration
  - Spoofing & bogons: uRPF is our IP-agnostic friend
  - 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