

---

# IPv6 Challenges for Intrusion Detection

---

Johannes B. Ullrich, Ph.D.  
jullrich@sans.edu  
SANS Technology Institute

---

## Outline

---

- IPv6 Introduction
- Extension Header Challenge
- Address Ambiguities
- Stateless Auto Configuration

## IPv6 Design Goals

- Scaling the Internet
  - More addresses
  - Simpler routing
- Adjusting to Modern Hardware
  - More memory
  - Larger address busses in CPUs

## Challenge #1: Addresses

- A host has more than one address
- It may not be clear which address is “preferred” (even between IPv4 and IPv6)
- Attacker may “multiplex” addresses
- Use of auto configured IPv6 addresses

## IPv6 Addresses

- 128 Bits: 64 bits for Network + 64 Bits for Interface

**2001:0DB8:CCCC:DDDD:EEEE:FFFF:0000:1111**

- Host will have multiple IP addresses

## EUI-64

- Uses MAC address to derive last 64 bits
- Regardless the network ID, the last 64 bits stay the same

## Privacy Enhanced / Temporary

- Last 64 bits are random
- Unlikely to collide
- Change once a day (configurable)
- Addresses kept for 7 days (just in case.. Again configurable)
- Link local still uses EUI-64

## DHCP / Static

- Still an option
- DHCPv6 very different from DHCPv4
- May not be supported
- Other addresses may still be used, or DHCP may just be used for DNS..

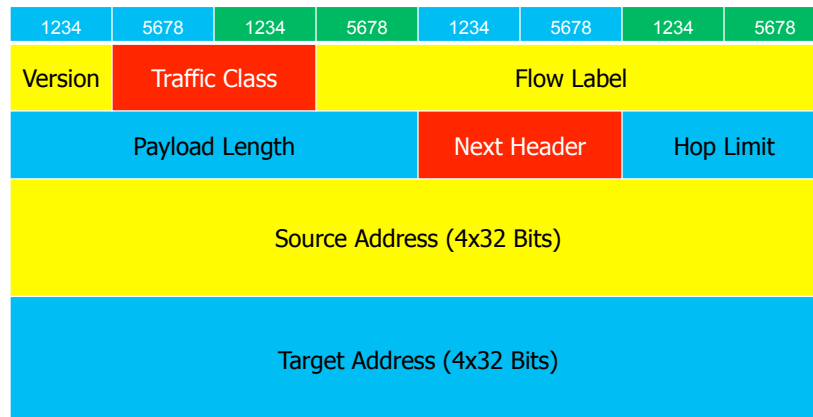
## IPv6 vs IPv4 Priority

- RFC suggests that IPv6 had priority over IPv4
- However, currently IPv6 turns out to be frequently broken / slow
- Operating systems and Applications come up with their own priority

## Happy Eyeballs

- OS X: Remembers if IPv6 timed out for specific addresses, and doesn't use IPv6 if auto configured tunnel
- Google Chrome: Gives IPv6 300 ms to make a connection

## IPv6 Header



## Compare to IPv4

- Simpler header
- No more flags (or any fragmentation information)
- No checksum
- Static 40 byte length

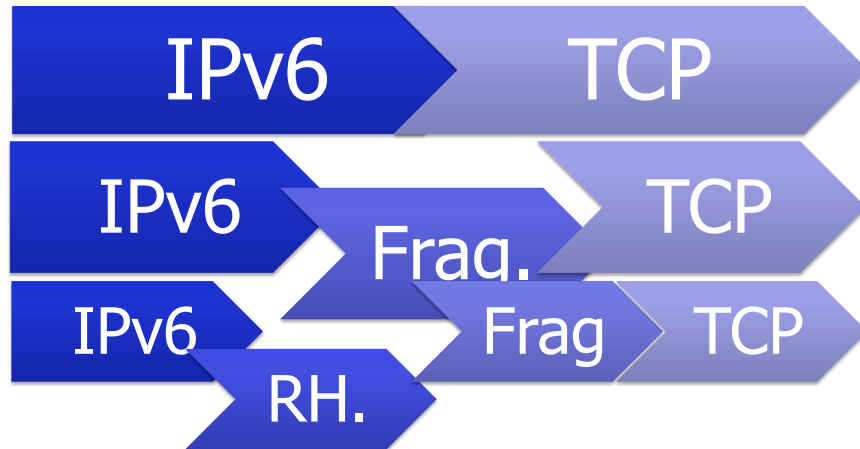
## Challenge #2: Header Size

- Some extension headers use flexible length
- Up to  $8 \times 256$  bytes (2 kBytes) per header
- Even one extension header may exceed local MTU
- Fragmentation?

## Extension Headers

- Many of the complexities are moved to extension headers
- Extension headers are optional
- Order is recommended but not enforced
- Can make IPv6 much more complex than IPv4

## Extension Headers



Title of Course - © 2008 SANS

15

## Extension Order Order

- Order is not fixed (“must accept headers in any order...”)
- Some may show up more than once
- Some are flexible in size

Title of Course - © 2008 SANS

16

## Challenge #3: Transport Protocol

- “Next Header” field in IPv6 header will not indicate TCP/UDP/ICMP...
- IDS has to find last extension header
- Extension headers can have variable size (up to 2kBytes)

## Finding Transport Protocol

- Older libpcap versions will crash in attempt to find last header
- Match becomes a lot harder (more CPU)
- No well defined order for extension headers
- Luckily: Extension headers not common

## Challenge #3: Routing Header

- Routing header is used for source routing
- IDS has to decode it to understand final destination of packet
- IP address destination just indicates next hop
- Space for up to 127 hops

## Example: TCP Reassembly

IPv6 Header	Routing Header	TCP Header	Payload
DST=A	-----	SN: 1	ABC
DST=A	DST=B	SN: 2	EXPLOIT
DST=A	-----	SN: 2	BEGNIGN

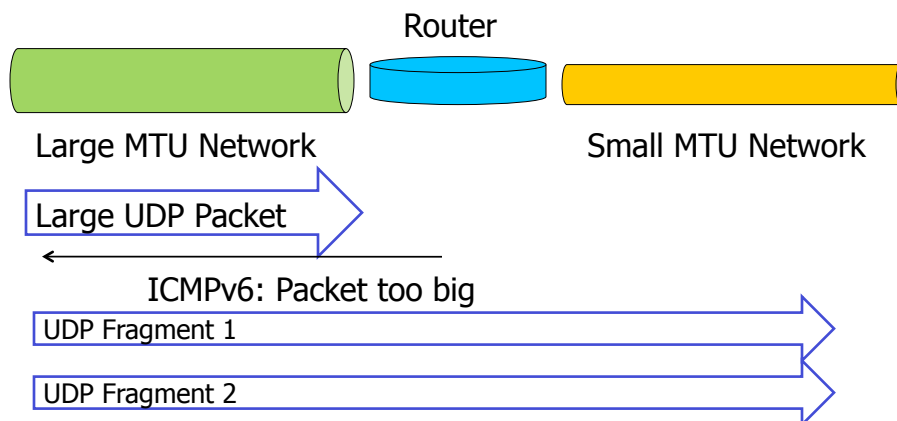
Possible solutions:

ABCEXPLOIT  
 ABCBEGNIGN

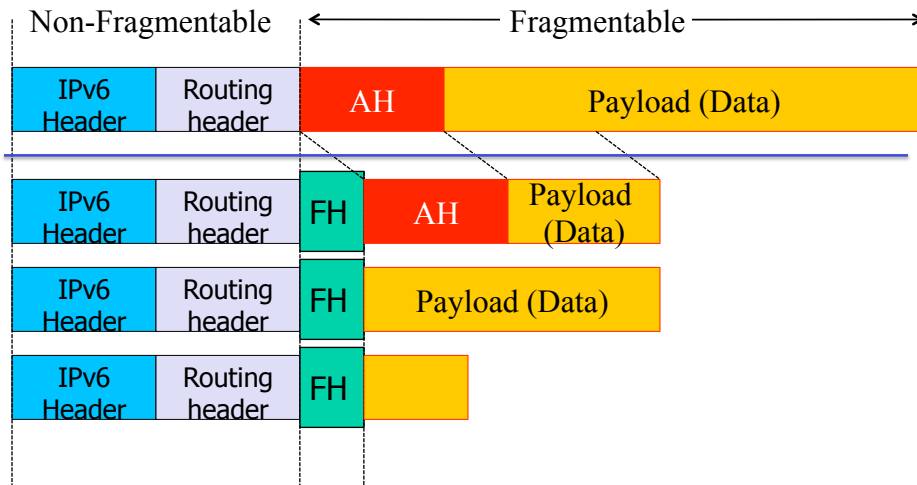
## Challenge #4: Fragmentation

- Fragmentation may still happen
- Done by source, not router
- Router will just send "fragmentation required" ICMP message
- Fragmentation header is used

## UDP Fragmentation (1)



## UDP Fragmentation (2)



Title of Course - © 2008 SANS

23

## Challenge

- Which headers are fragmented (or not?)
- All fragments but the last one must have the same size
- But who reads the RFC (other than developers making bad assumptions)

Title of Course - © 2008 SANS

24

## Challenge #5: ICMPv6

- ICMPv6 does a lot more
- Replaces ARP
- Used for auto configuration
- More complex protocol than ICMPv4

## Neighbor Discovery

- Protocol to replace ARP
- Uses autoconfigured link local addresses
- Very similar to ARP: same security issues

## Router Advertisements

- “DHCP Lite”
- Used to configure IP address
- Router advertises first 64 bits, host picks the next 64 bits
- In some cases, a DNS server and other settings may be configured

## Fake routers

- Just like a rogue DHCP server
- For DHCP we got DHCP Snooping in switches
- For Router Advertisements, we got “RAGuard” in a few switches

## Router Advertisements

- Switch needs to detect router advertisements
- Sounds easy: "Next Header" is ICMPv6 and ICMPv6 Type is "Router Advertisement"

## RAGuard

- Feature is some modern switches (few) to detect Router Advertisements and limit them to authorized ports.
- Not widely implemented (unlike DHCP Snooping)

## RAGuard Bypass

- ICMPv6 packets may include extension headers
- "Next Header" field in IPv6 header may not indicate ICMPv6
- Switch has to look for last header

## RAGuard Bypass

- ICMPv6 may be fragmented
- Switch has to reassemble fragments to figure out if packet is a RA
- Has to do it for all fragments where the NH is not a transport header

## Update Standard?

- Some effort under way to clean up standard
- Do not allow any other headers than ICMPv6 for RA
- Do not allow fragmented RA

## Tunnels

- A whole different talk...
- Really an IPv4 problem, not an IPv6 problem
- Can lead to bad assumptions: NAT protects your hosts from inbound traffic?

## Summary

- IPv6 introduces interesting new complexities
- Makes intrusion detection on IP layer interesting again
- Carefully test security features for IPv6 support!

## Thanks

jullrich@sans.edu

<http://isc.sans.edu>

Twitter: @johullrich

Daily podcast:[http://isc.sans.edu/  
podcastdetails.html](http://isc.sans.edu/podcastdetails.html)

Please consider submitting logs!