IPv6 extension headers in Routing Security

China Future Internet Engineering Center
Haisheng Yu (Johnson)
yuhaisheng1@gmail.com

2021/6

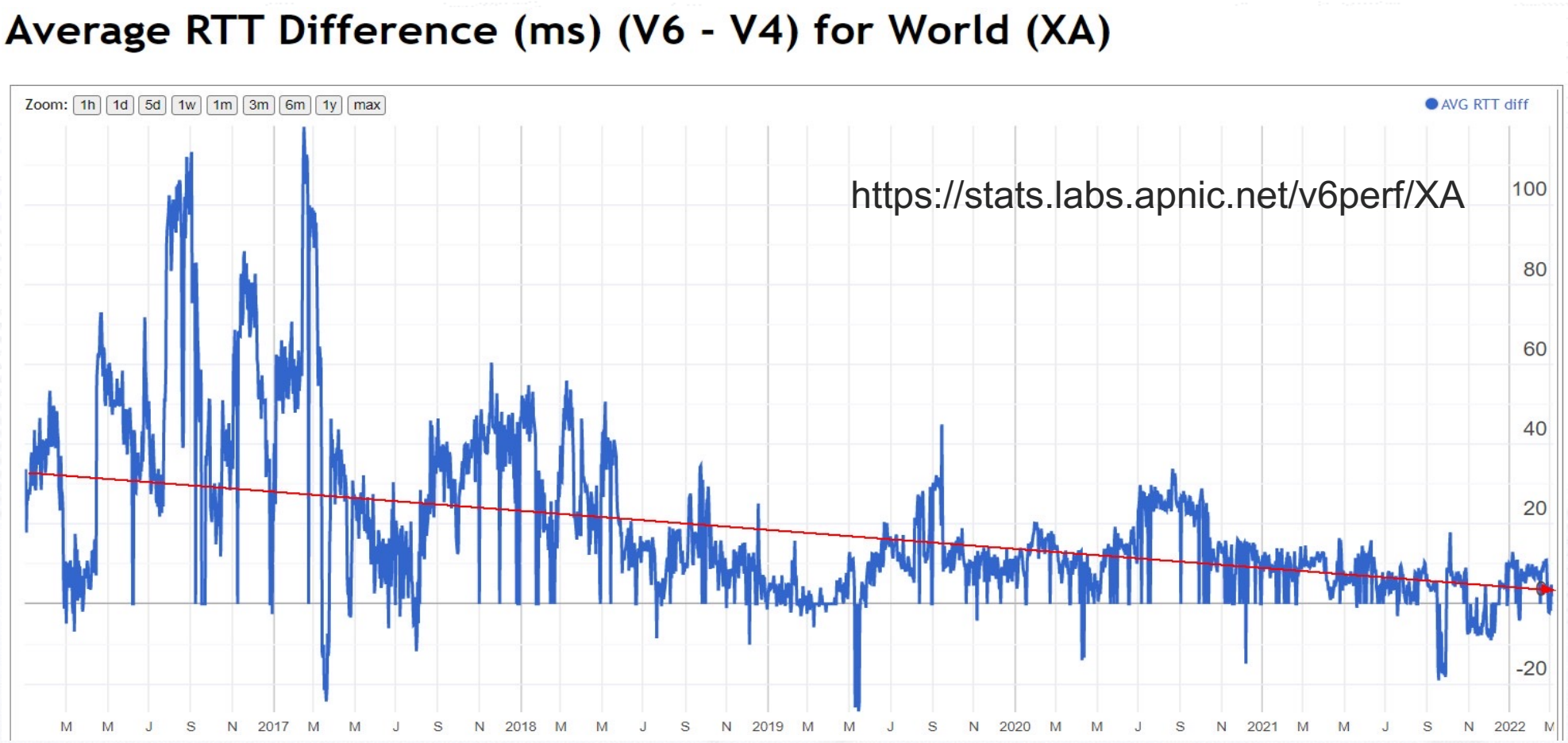
CONTENTS

Definition of performance

1. the reliability of the protocol
- All connection attempts successful
- higher connection failure rates in one protocol or the other?
- Is middleware that drops IP packets based on the IP protocol deployed on the network path?

2. the round-trip time
- Same two endpoints are involved, one protocol may use a different network path than another
- The peering and transport arrangements used between providers can vary from protocol to protocol
- There are also more subtle issues with packet processing within routers

IPv6 Performance Challenge 1: IPv6 RTT Improving but still 2.5ms Higher than IPv4

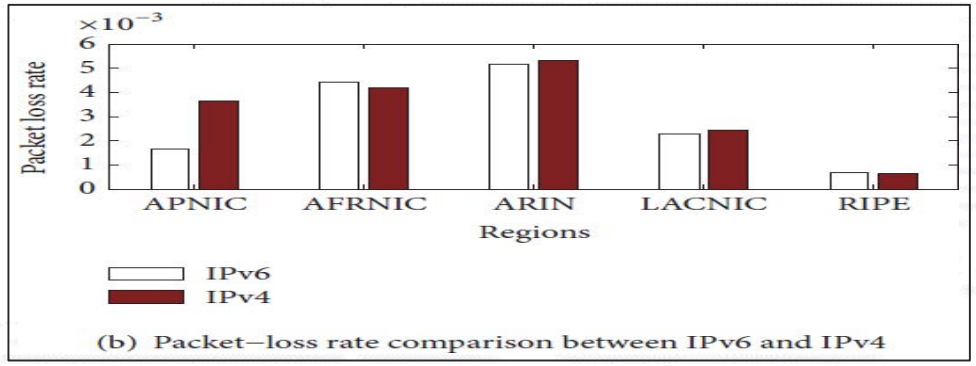


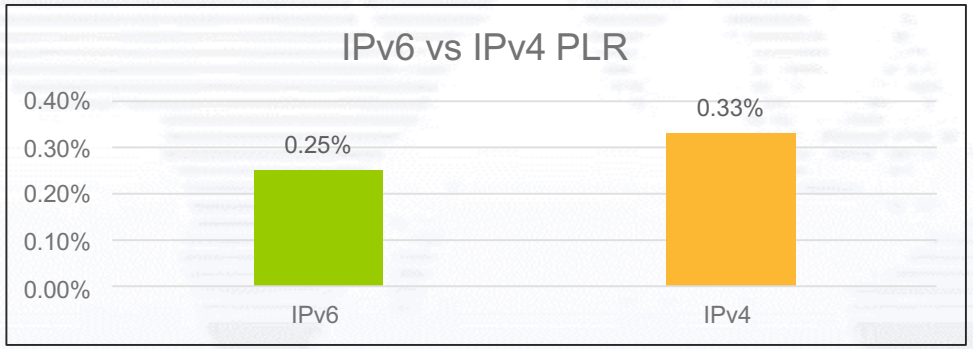
- What are top-3 factors leading to IPv6 RTT improvement?

Refer to Xipeng Xiao's report at IETF-113

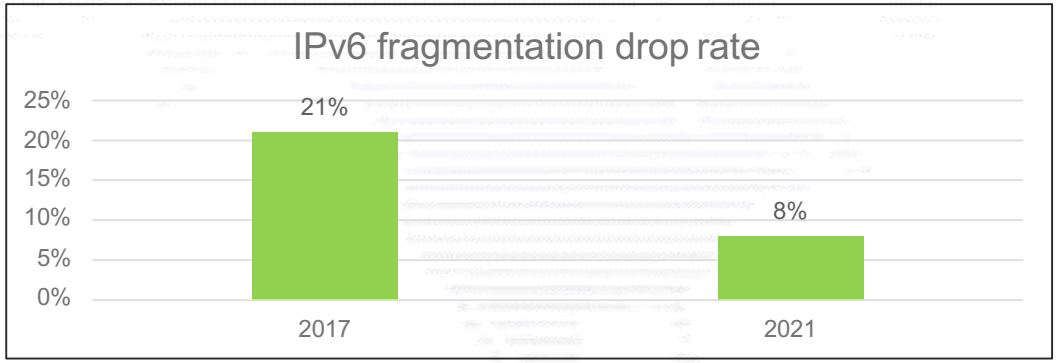
Performance Challenge 2: IPv6 Packet Loss Rate Likely Higher

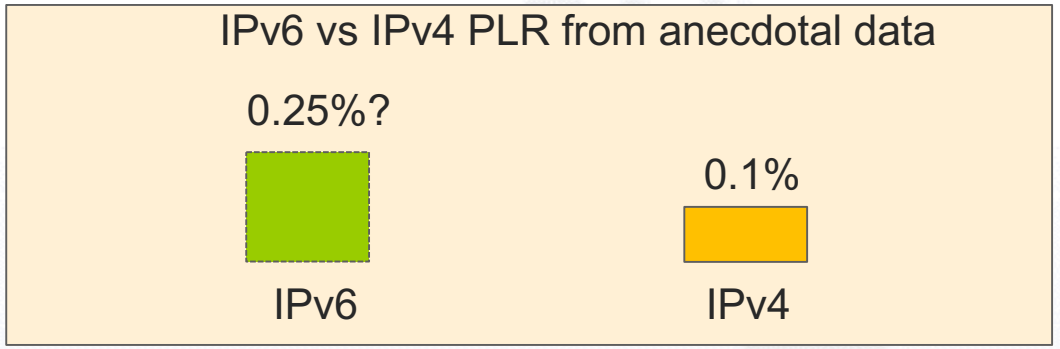
[Hindawi] reported lower IPv6 PLR than IPv4, based on 1-week measurement from China.





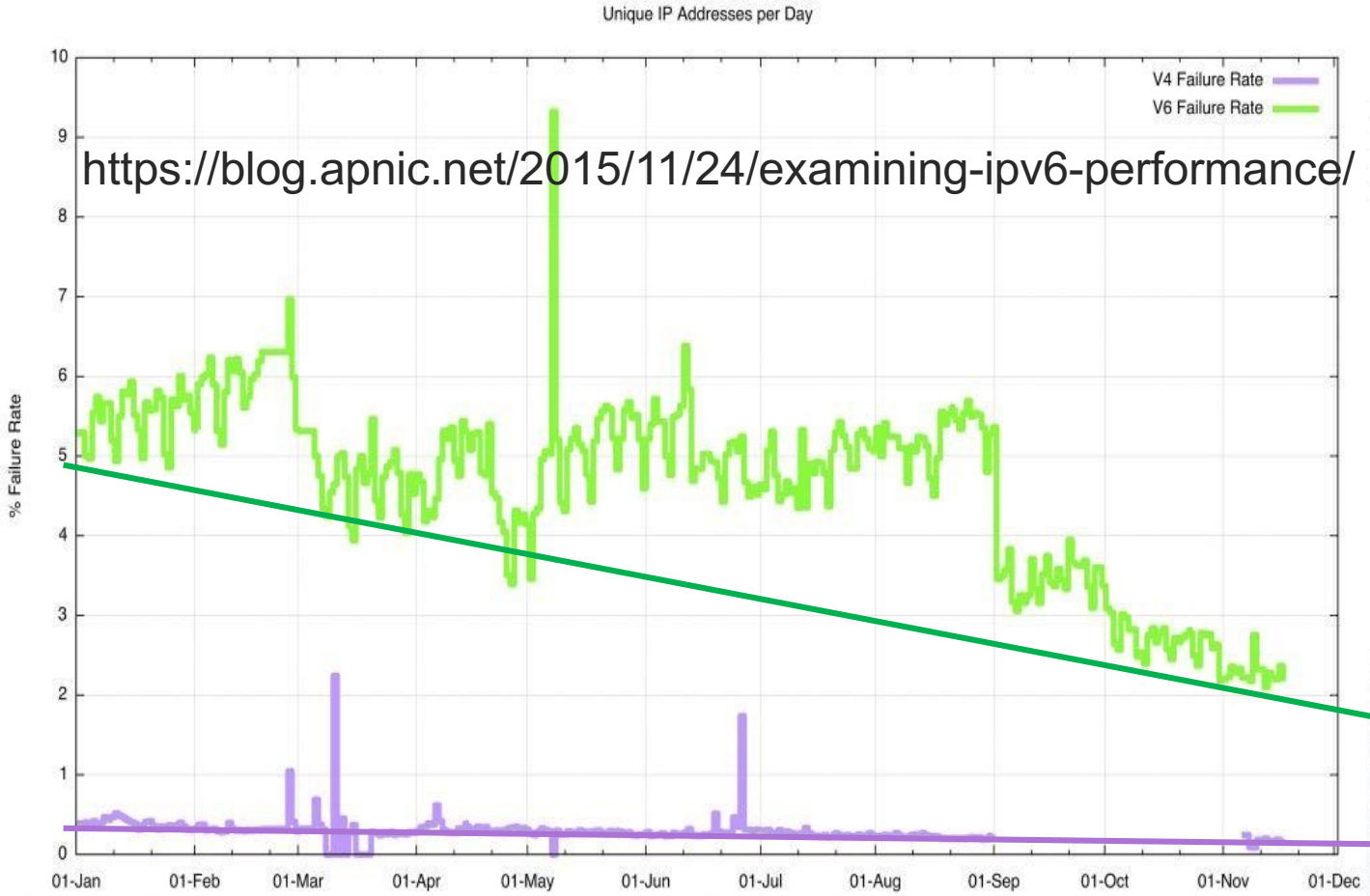
[RFCs 7872/9098] reported very high PLR for IPv6 packets with EHs. Combined with anecdotal data, we believe IPv6 PLR is higher





- How much does high IPv6 packet loss due to EHs, fragmentation, filtering contribute to overall IPv6 PLR?
- Should we measure IPv6 PLR and analyze the causes?

Performance Challenge 3: IPv6 TCP Failure Rate Higher



https://blog.apnic.net/2015/11/24/examining-ipv6-performance/

APNIC

- IPv6: 0.96%
- IPv4: 0.25%

TCP Connection Failure Rates for IPv6 & IPv4, in 2015 in Mar. 2022

- Is higher IPv6 TCP failure rate due to higher IPv6 PLR?
- Should we measure failure rate for QUIC now?

CONTENTS

IPv6 vs IPv4

In some respects, IPv6 is designed to be a more processor-friendly protocol than IPv4. In particular, IPv4 headers are variable length, while IPv6 headers are fixed length. This is very helpful. It also organizes its options so that the transit router doesn't even need to try to parse options that are only relevant to the destination node.

In other respects, IPv6 presents a bigger challenge than IPv4: IPv6 has more options due to its greater scalability. The IPv6 header chain can get quite large, and can be large enough to trigger some of the above problems when the headers exceed the capacity of fast memory for the forwarding engine to store them.

IPv6 extension header list and execution order

Basic header ipv6 header

0 Hop-by-Hop Options header

60 Destination Options header Destination Options header

43 Routing header Routing header

44 Fragment header Fragment header

51 Authentication header Authentication header

50 Encapsulating security payload header

59 ICMPv6

60 Destination option header

Upper-layer header upper-layer header (TCP=6 /UDP=17)

Potential threats of IPv6 extension headers

- Extension headers (other than the Hop-by-Hop Options header) are not processed, inserted or removed by any node
- The delivery path of the packet until the packet reaches the node"
- Problem or threat: shouldn't firewalls (stateful/stateless) check them?
- But the destination node MUST accept and process the extended header, "any order and any number of occurrences in the same packet"
- Problem or threat: If the extension header is too complex, it will put a lot of processing pressure on the destination node agent

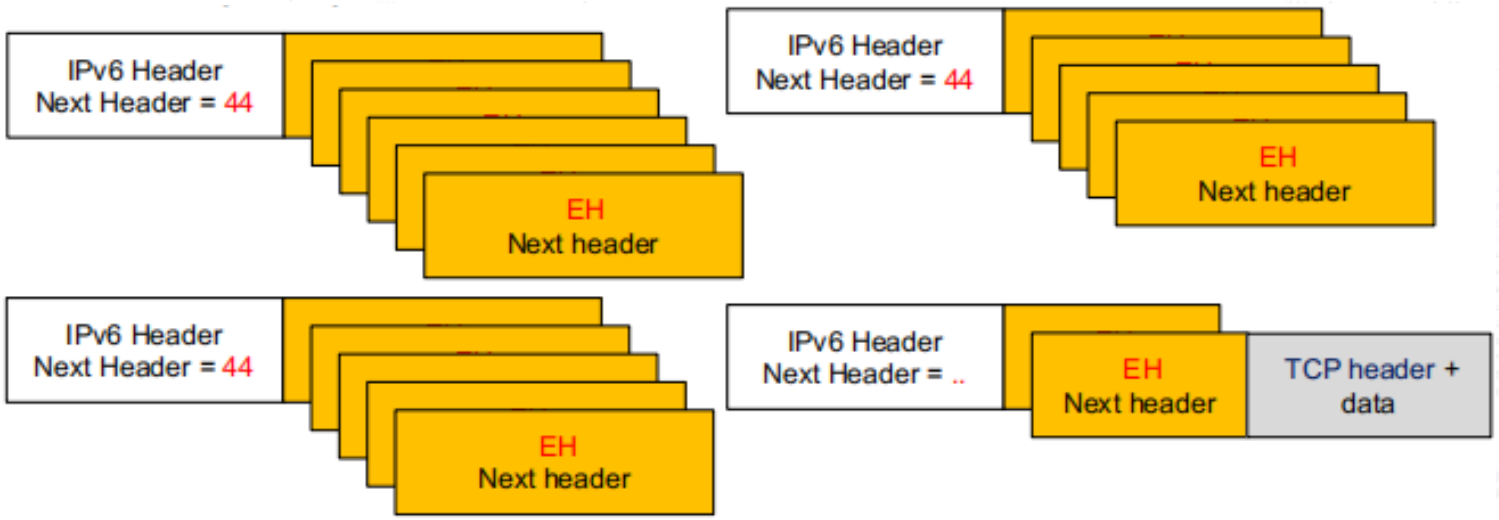
Potential threats to IPv6 extension headers

- Unlimited number of EHs: the number of options in the option header
- Unlimited number of options for Hop-by-Hop extension headers
- The order of EH is not defined (only one recommendation)
- RFC2460/8200 "It is recommended that these headers appear in order"

Potential threats to IPv6 extension headers

- Use extension headers to exchange information, interactive information cannot be detected
- If you want to solve it, throw away the unknown extension header, which means you need to detect the extension header, which does not conform to the protocol

Potential threats to IPv6 extension headers



- Send packets with lots of EH
- The EH chain itself is fragmented (L4 information may appear in the Nth shard)
- Overwhelm the target node (DOS)
- Avoid IPS/IDS/Firewall

Potential threats to IPv6 extension headers

- Should we discard all IPv6 fragments?
- How do services like DNSSEC work?
- RFC7112: - "When a host fragments an IPv6 datagram, it MUST include the entire IPv6 header chain in the first fragment" • Check and remove
- RFC8200: - "The extension header, if any, and the upper layer header must be in the first fragment

Existing IPv6 hop-by-hop options

- Hop-by-hop forwarding options:
- PAD Options: PAD1 and PADn [RFC8200]
- Jumbo Payload [RFC2675]
- RPL Option [RFC6553]
- Common Architecture Label 1Pv6 Security Option [RFC5570]
- SMF Option [RFC6621]
- MPL Option [RFC7731]
- DFF Option [RFC6971]
- MTU Option [I-D.ietf-6man-mtu-option]
- AltMark Option [I-D.ietf-6man-ipv6-alt-mark]
- In-situ OAM [I-D.ietf-ippm-ioam-ipv6-options]

- Hop-by-hop control options:
- Router Alert Option [RFC2711]
  Quickstart Option [RFC4782]

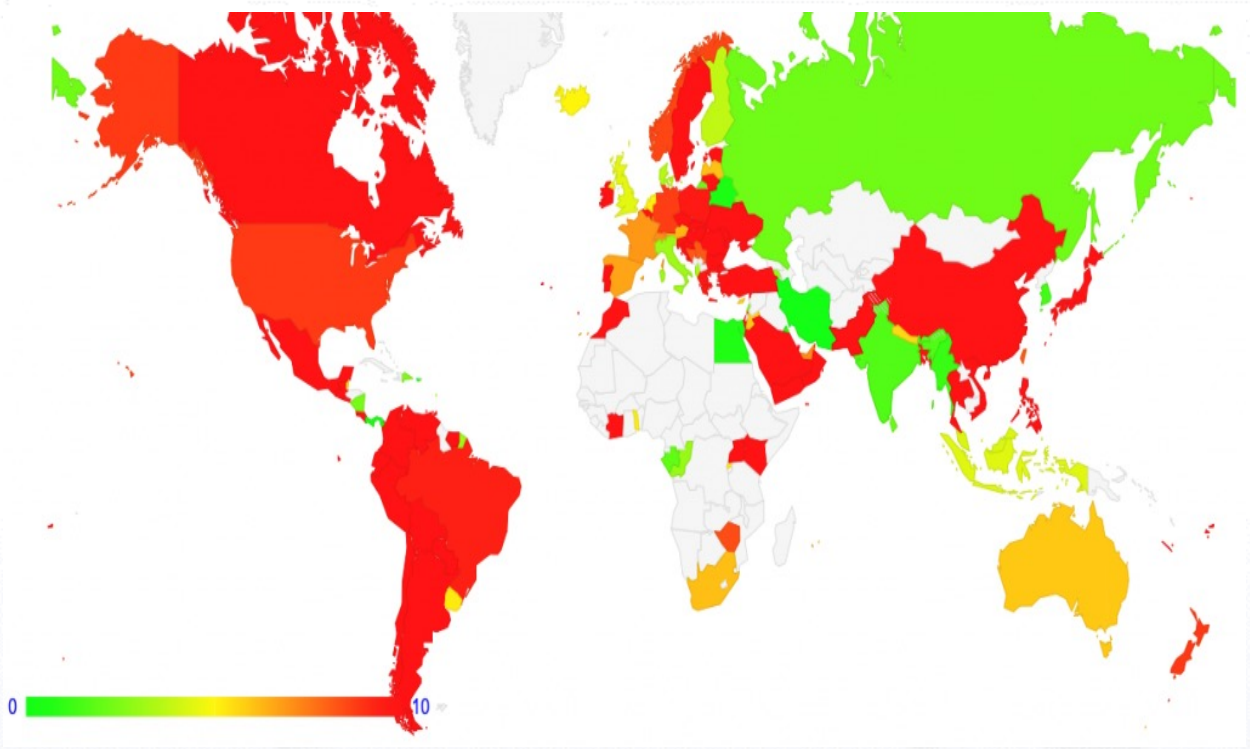
Path MTU discovery as an HBH function

- IPv6 packets carrying this HBH option are not arbitrarily discarded by devices on the path or by the destination host.
- All forwarding devices recognize this HBH option and will update the Min Path MTU field when forwarding IPv6 packets that contain this HBH extension header.
- All IPv6 hosts recognize this HBH option and receivers will echo all received path MTU HBH options values back to the sender as determined by the control flag.
- All IPv6 hosts will make local adjustments to their stored value of path MTU in accordance with this received MTU information.
- All IPv6 protocol implementations need to support a socket option to allow upper layer protocols to request this path MTU probe function.

Suggested HBH Handling Procedure

- Source HBH option header encapsulation. When the source HBH option header is encapsulated, if there is no HBH option header to be filled, it is marked as passed by default, and when there is HBH option to be filled, it is marked as need to be processed. The information to be carried in the HBH option header needs to be classified first, then encapsulated into control options or forwarding options, and finally encapsulated in different data packets.
- The edge nodes of the network. Edge nodes should check whether the packet contains an HBH header with control options or and forwarding options. Packets with forwarding options should be allowed by the ACL, and packets with only control options are handled at the discretion of the node.

IPv6 fragmentation loss in 2021



Distribution of IPv6 fragmentation drop rates per economy

Code	Region	Fragmentation drop rate	IPv6 samples
XA	World	6.68%	23,209,746
XC	Americas	10.94%	6,274,581
XB	Africa	9.50%	126,575
XE	Europe	9.33%	2,532,014
XF	Oceania	6.62%	75,380
XG	Unclassified	5.39%	21,213
XD	Asia	4.29%	14,179,983

IPv6 Fragmentation drop rate per region in 2021

Source:https://blog.apnic.net/2021/04/23/ipv6-fragmentation-loss-in-2021/

Reasons for IPv6 fragmentation loss

- Firewalls are often configured to drop fragments.
- Network equipment may be configured to drop all IPv6 packets that contain Extension Headers.
- Network equipment may pass packets with Extension Headers to a ‘slow path’ processing, and this may have an associated queue build-up and cause sporadic loss
- There may be path MTU issues where larger packets are being dropped.

CONTENTS

Why is the usage of IPv6 extension headers low?

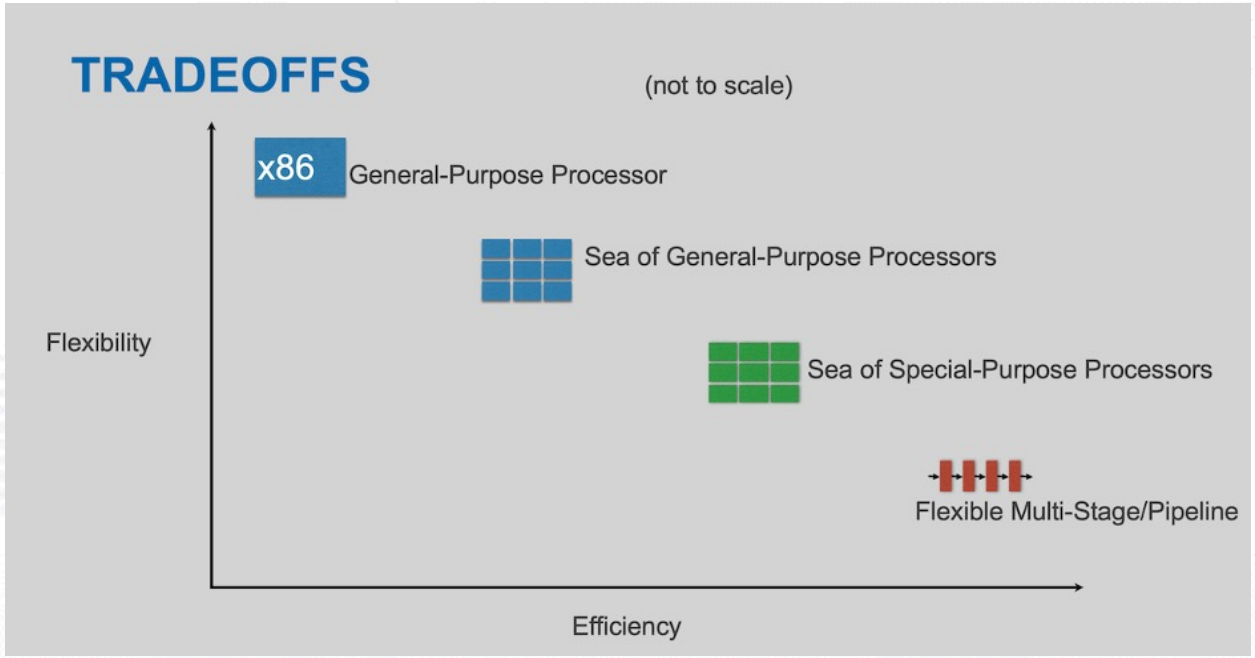
- Extension header (EH) requires complex processing and becomes a potential DoS carrier.
- Since EH is a DoS carrier, network operators deploy access control lists (ACLs) to drop packets containing EH.
- Since network operators deploy access control lists (ACLs) that drop packets containing EH, network engineers no longer define new EH applications.
- With network engineers no longer defining new EH applications, there is little incentive to fix the implementation issues that made EH a DoS carrier.

The flexibility of TLVs VS the fixedness of chips

- Fixed header length makes parsing easier
- Despite what ‘everyone knows’, it’s not crucial for fields to be sized to a power-of-two, or even to be word-aligned.
- Fixed locations for fields is important though, and it’s helpful for the overall header length to be a multiple of 32 bits. One implication of this is that TLVs in headers that must be parsed hop-by-hop are costly.
- It’s very tempting for protocol designers to throw an optional TLV field into everything — who couldn’t love future-proofing? The answer is, people who have to check for TLV presence in the fast path, and potentially parse an indeterminate number of TLVs, that’s who!

Source： https://blog.apnic.net/2020/06/04/modern-router-architecture-and-ipv6/

Processor tradeoffs



- On the left, you have a general-purpose processor
- In the middle, we have a couple of NPU variants
- And at the far end of the spectrum, we have the pipeline processor

As a router' s flexibility decreases, its efficiency increases. The trick for vendors is to balance cost and performance.

Source:https://blog.apnic.net/2020/06/04/modern-router-architecture-and-ipv6/

Suggestion

- The forwarding decision must fit in the key data
- Fixed header lengths make parsing easier
- Use an established header in a novel way instead of inventing a new one
- Manage header size
- Determine the order in which extension headers appear, let pipeline processors parse the packet before starting any lookup, and avoid any additional indirection inserted into this parsing process.
- Use established headers and options in novel ways as much as possible, rather than inventing new headers and options

Thanks !