Internet Engineering Task Force (IETF) IPv6 News

What are the new IPv6-related RFC / drafts since 2020 ?

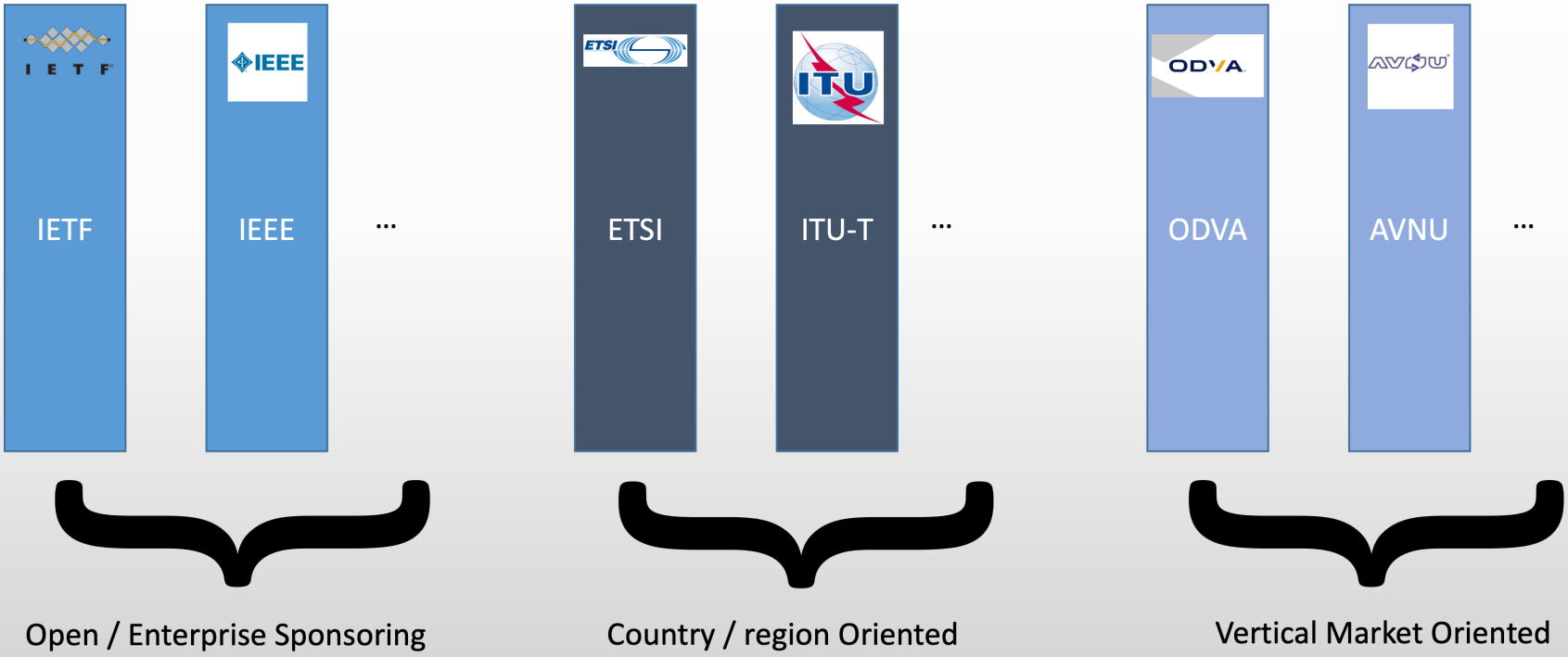
Eric Vyncke
Distinguished Engineer evyncke@cisco.com, IETF Area Director
April 2022

The next slides are my personal view and does not represent Cisco or IETF views

How is the IETF organized ?

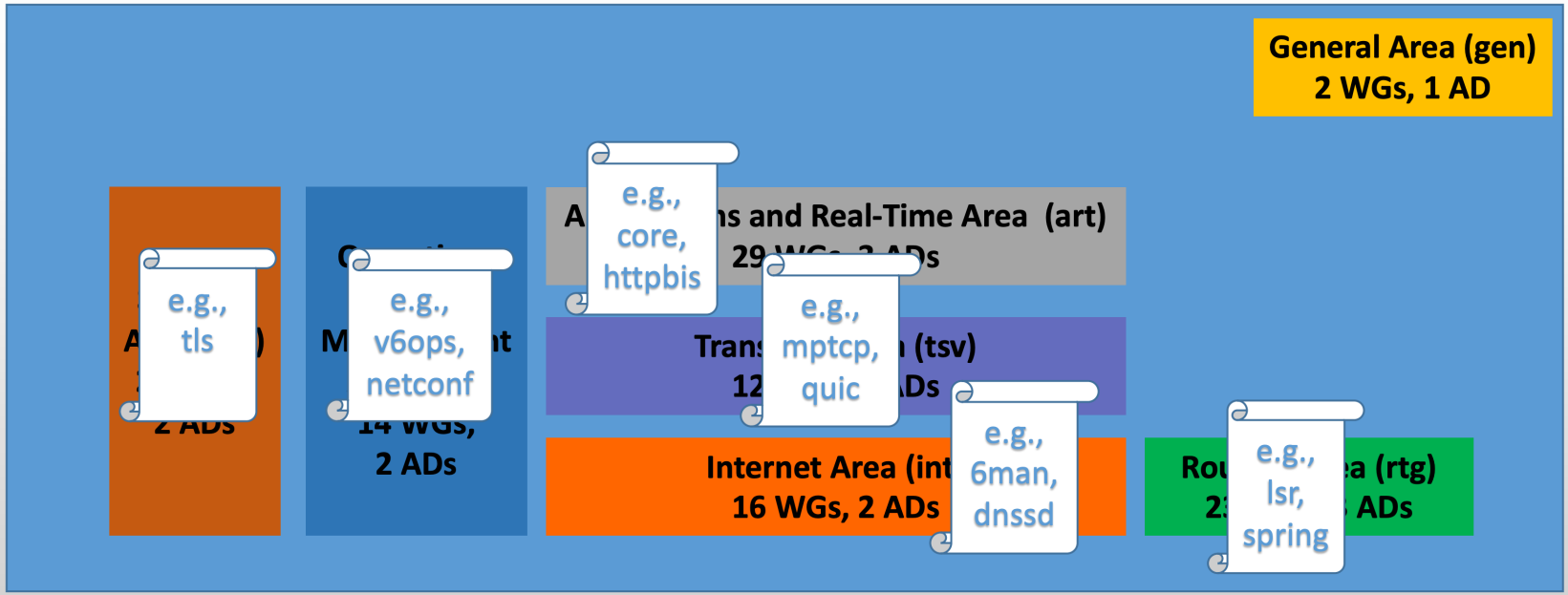
Source: https://datatracker.ietf.org/meeting/103/materials/slides-103-edu-sessm-internet-area-overview-00

Standards Developing Organizations (SDOs)



The IETF is divided in Areas

Used to change often, very stable for the last 10+ years



int active WGs (17)

Group	Responsible AD	Name	Chairs
6lo	Erik	IPv6 over Networks of Resource-constrained Nodes	Shwetha Bhandari, Carles Gomez
6man	Erik	IPv6 Maintenance	Bob Hinden, Jen Linkova, Ole Trøan
6tisch	Erik	IPv6 over the TSCH mode of IEEE 802.15.4e	Pascal Thubert, Thomas Watteyne
add	Éric	Adaptive DNS Discovery	Glenn Deen, David Lawrence
dhc	Éric	Dynamic Host Configuration	Bernie Volz, Timothy Winters
dmm	Erik	Distributed Mobility Management	Sri Gundavelli, Dapeng Liu, Satoru Matsushima
dnssd	Éric	Extensions for Scalable DNS Service Discovery	Chris Box, David Schinazi
dprive	Éric	DNS PRIVate Exchange	Brian Haberman, Tim Wicinski
drip	Éric	Drone Remote ID Protocol	Mohamed Boucadair, Daniel Migault
homenet	Éric	Home Networking	Stephen Farrell, Kiran Makhijani
intarea	Éric	Internet Area Working Group	Wassim Haddad, Juan-Carlos Zúñiga
ipwave	Erik	IP Wireless Access in Vehicular Environments	Carlos Bernardos, Russ Housley
lpwan	Éric	IPv6 over Low Power Wide-Area Networks	Alexander Pelov, Pascal Thubert
lwig	Erik	Light-Weight Implementation Guidance	Zhen Cao, Mohit Sethi
madinas	Éric	MAC Address Device Identification for Network and Application Services	Carlos Bernardos, Juan-Carlos Zúñiga
ntp	Erik	Network Time Protocols	Karen O'Donoghue, Dieter Sibold
tictoc	Erik	Timing over IP Connection and Transfer of Clock	Karen O'Donoghue, Yaakov Stein

IPv6-related Working Groups

6MAN: IPv6 Maintenance

- Defines / controls the Evolution of IPv6
  - And prepare for IPv4 sunset
- It is the design authority for extensions and modifications to the IPv6 protocol
- Sociological dimension
  - Address Privacy
  - Freedom to form an address
- Political dimension
  - Conservationists care for a stable protocol to encourage deployments
  - Progressists want the protocol to evolve, else it dies (e.g., Segment Routing)

6lo and LPWAN

- Low Power Link layer crowds
  - BLE, BACNet, NFC, PowerLine, ZWave, 802.15.4, LoRaWAN, NB IOT, SIGFOX…
- IOT: new Internet use cases
  - Metering and Automation, Industrial Internet
- Redefining some classical operation
  - IPv6 ND
- Providing new solutions to
  - Fragmentation for small MTUs
  - Header Compression

IPWAVE: IP Wireless Access in Vehicular Environments

- V2V and V2I use-cases where IP is well-suited as a networking technology
  - develop **an IPv6-based solution** to establish direct and secure connectivity between a vehicle and other vehicles or stationary systems.
- Specify the mechanisms for transmission of **IPv6 datagrams** over IEEE 802.11-OCB mode.

V6OPS: IPv6 Operations

- Operation crowd practicing the technology
- Feeds back on the protocol in the real world
- Produces Best Practice

- When real world experience meets academics ☺
- Really worth reading/learning from…

Recent published RFC

Internet Engineering Task Force (IETF)
Request for Comments: 8754
Category: Standards Track
ISSN: 2070-1721

C. Filsfils, Ed.
D. Dukes, Ed.
Cisco Systems, Inc.
S. Previdi
Huawei
J. Leddy
Individual
S. Matsushima
SoftBank
D. Voyer
Bell Canada
March 2020

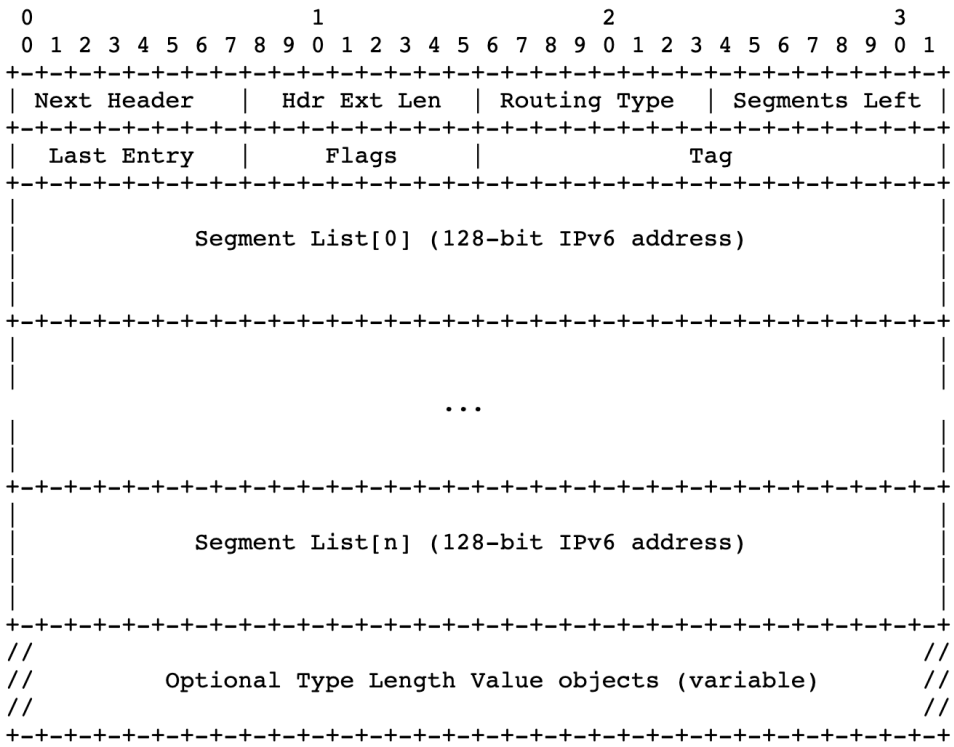
IPv6 Segment Routing Header (SRH)

Abstract

Segment Routing can be applied to the IPv6 data plane using a new type of Routing Extension Header called the Segment Routing Header (SRH). This document describes the SRH and how it is used by nodes that are Segment Routing (SR) capable.

Routing Header is Alive and Kicking !

- With security added of course
  - HMAC TLV
  - Infrastructure ACL on routing header type == 4 (to protect an internal “limited domain” – see JAMES presentation)
- Can be used for traffic engineering to enforce a path between routers or Virtual Network Functions (NFV)



Going beyond traffic engineeing

- Legacy/current traffic engineering
  - Install processing instructions (QoS, security, encaps/decaps) in the path
  - Each node must classify ingress packets and apply the above instructions

- What if the instructions were part of the packet ?
  - I.e., a small program in packets
  - E.g., using the IPv6 addresses in segment routing header (SRH) as a line of code in addition to routing ?
  - => network programming !

Internet Engineering Task Force (IETF)
Request for Comments: 8986
Category: Standards Track
ISSN: 2070-1721

C. Filsfils, Ed.
P. Camarillo, Ed.
Cisco Systems, Inc.
J. Leddy
Akamai Technologies
D. Voyer
Bell Canada
S. Matsushima
SoftBank
Z. Li
Huawei Technologies

February 2021

Segment Routing over IPv6 (SRv6) Network Programming

Abstract

The Segment Routing over IPv6 (SRv6) Network Programming framework enables a network operator or an application to specify a packet processing program by encoding a sequence of instructions in the IPv6 packet header.

Each instruction is implemented on one or several nodes in the network and identified by an SRv6 Segment Identifier in the packet.

IPv6 Address as a “Line of Code”

- Each IPv6 address in SRH can then be decomposed in
  - LOCator: to route the packet to the next processing node
  - FUNCTion: a standard instruction (layer-2/3 forward on interface, decaps, ...)
  - ARGument(s): the arguments for the instruction above

- Note: segments in SRH look like IPv6 and are often named “SID” (for segment ID)
  - See also: draft-krishnan-6man-sids for a discussion on the relationship between RFC 8754 & 8986 and RFC 4291 (IPv6 addressing architecture)

IPv6 Address as line of code, an example

- LOCator
  - ISP wants to use 2001:db8::/32 as “net-pgm” block prefix
  - ISP uses 2001:db8:*n*::/48 to identify node *n*
- FUNCTion
  - 0x0100 for “End.DT2M: Decapsulation and L2 Table Flooding”
- ARGument
  - 0xcafe: for a specific set of outgoing interface(s) for the flooding
- => 2001:db8:123:100:cafe::/128 to “code” the DT2M behavior in node 123
- *Signaling and/or controllers are required to propagate those values*

From: draft-ietf-6man-icmp-limits-08 Proposed Standard
Internet Engineering Task Force (IETF) T. Herbert
Request for Comments: 8883 Intel
Category: Standards Track September 2020
ISSN: 2070-1721

ICMPv6 Errors for Discarding Packets Due to Processing Limits

Abstract

Network nodes may discard packets if they are unable to process protocol headers of packets due to processing constraints or limits. When such packets are dropped, the sender receives no indication, so it cannot take action to address the cause of discarded packets. This specification defines several new ICMPv6 errors that can be sent by a node that discards packets because it is unable to process the protocol headers. A node that receives such an ICMPv6 error may use the information to diagnose packet loss and may modify what it sends in future packets to avoid subsequent packet discards.

Node can signal “Cannot process this ext header”

- RFC 8883 adds new ICMPv6 codes for “parameter problem” error message to ease troubleshooting

Code	Name	Reference
0	erroneous header field encountered	
1	unrecognized Next Header type encountered	
2	unrecognized IPv6 option encountered	
3	IPv6 First Fragment has incomplete IPv6 Header Chain	[RFC7112]
4	SR Upper-layer Header Error	[RFC8754]
5	Unrecognized Next Header type encountered by intermediate node	[RFC8883]
6	Extension header too big	[RFC8883]
7	Extension header chain too long	[RFC8883]
8	Too many extension headers	[RFC8883]
9	Too many options in extension header	[RFC8883]
10	Option too big	[RFC8883]

https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-codes-5

Internet Engineering Task Force (IETF)
Request for Comments: 9098
Category: Informational
ISSN: 2070-1721

F. Gont
SI6 Networks
N. Hilliard
INEX
G. Doering
SpaceNet AG
W. Kumari
Google
G. Huston
APNIC
W. Liu
Huawei Technologies

September 2021

Operational Implications of IPv6 Packets with Extension Headers

Abstract

This document summarizes the operational implications of IPv6 extension headers specified in the IPv6 protocol specification (RFC 8200) and attempts to analyze reasons why packets with IPv6 extension headers are often dropped in the public Internet.

RFC 9098 Operational Implications of IPv6 Packets with Extension Headers

- Impact of long ext headers chain on operations
  - Layer-4 and payload are difficult to find and parse
  - Can slow down the forwarding
- Examples
  - Infrastructure ACL or QoS
  - Equal Cost Multi Path (ECMP)
  - Intrusion Prevention Systems
  - Firewalls

From: draft-ietf-opsec-v6-27 Informational
Internet Engineering Task Force (IETF) É. Vyncke
Request for Comments: 9099 Cisco
Category: Informational K. Chittimaneni
ISSN: 2070-1721

M. Kaeo
Double Shot Security
E. Rey
ERNW
August 2021

Operational Security Considerations for IPv6 Networks

Abstract

Knowledge and experience on how to operate IPv4 networks securely is available, whether the operator is an Internet Service Provider (ISP) or an enterprise internal network. However, IPv6 presents some new security challenges. RFC 4942 describes security issues in the protocol, but network managers also need a more practical, operations-minded document to enumerate advantages and/or disadvantages of certain choices.

Internet Engineering Task Force (IETF)
Request for Comments: 9131
Updates: 4861
Category: Standards Track
ISSN: 2070-1721

J. Linkova
Google

October 2021

Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers

Abstract

Neighbor Discovery (RFC 4861) is used by IPv6 nodes to determine the link-layer addresses of neighboring nodes as well as to discover and maintain reachability information. This document updates RFC 4861 to allow routers to proactively create a Neighbor Cache entry when a new IPv6 address is assigned to a node. It also updates RFC 4861 and recommends that nodes send unsolicited Neighbor Advertisements upon assigning a new IPv6 address. These changes will minimize the delay and packet loss when a node initiates connections to an off-link destination from a new IPv6 address.

GRAND in a snapshot

- Problem:

1. A node starts sending traffic via the router,
2. the return flow arrives to the router,
3. no neighbor cache entry => trigger address resolution
4. packets dropped (cached) until address resolution completes.

- Solution:

1. Nodes advertise their addresses by sending unsolicited NAs
2. Routers create STALE entries

Some RFC are special...

- Expect not-too-serious RFC published on 1st of April 2022...
  - Usual RFC have a publication date such as “April 2022”
  - Those RFC are date “1st April 2022”
    - RFC 3514 “The Security Flag in the IPv4 Header”
    - RFC 1149 “Standard for the transmission of IP datagrams on Avian Carriers”
    - RFC 2549 “IP over Avian Carriers with Quality of Service”
    - RFC 5514 “IPv6 over Social Networks”

- Expecting some new ones today !

Recent IETF drafts (I-D)
I.e., not yet standards, no consensus yet, but adopted by a WG

6MAN main topic: extension headers

- draft-ietf-6man-eh-limits
- draft-ietf-6man-hbh-processing
- draft-ietf-6man-mtu-option
- draft-ietf-6man-enhanced-vpn-vtn-id

draft-ietf-6man-eh-limits

"This specification defines various limits that may be applied to receiving, sending, and otherwise processing packets that contain IPv6 extension headers. "

- Based on Postel's law "*Be conservative in what you send, liberal in what you receive*"
- Limits on EH number, length per EH, length of EH chain, number of options in EH, ...
  - A host MUST NOT send more than 8 non-padding options in Destination Options
  - A host MUST NOT send a packet with an extension header larger than 64 bytes
  - An intermediate node MUST be able to correctly forward packets that contain an IPv6 header chain of 104 or fewer bytes
  - ...

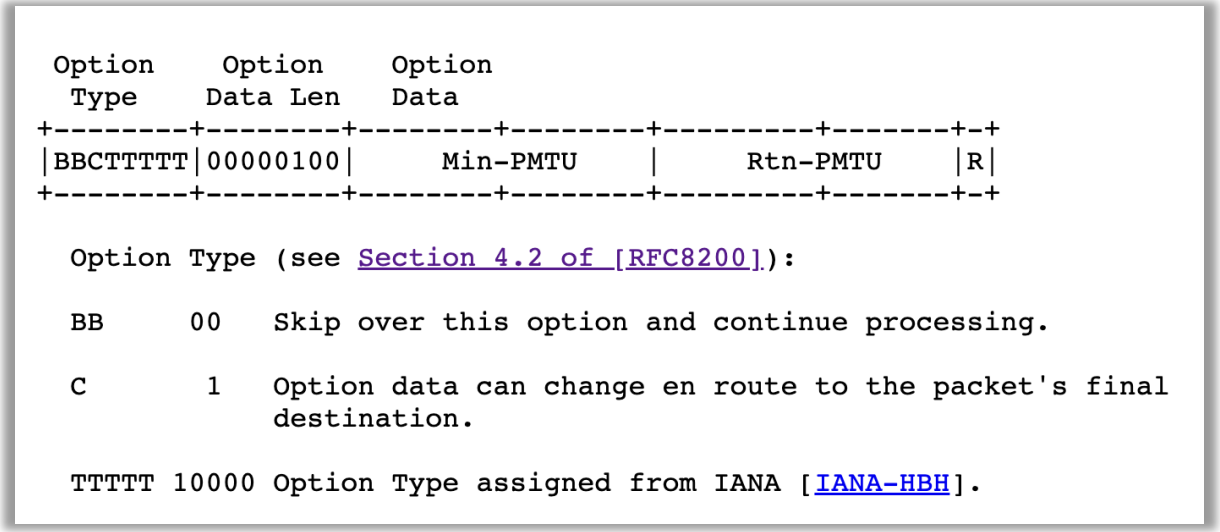
draft-ietf-6man-hbh-processing

"It modifies the procedures specified in the IPv6 Protocol Specification (RFC8200) to make processing of IPv6 Hop-by- Hop options practical with the goal of making IPv6 Hop-by-Hop options useful to deploy and use in the Internet."

- This IETF draft hopes to enforce the processing of HbH over the Internet
  - "This document updates [RFC8200] that a node **MUST** process the first Option in the Hop-by-Hop Header at full forwarding rate the (e.g. on the router's Fast Path) and **MAY** process additional Hop-by-Hop Options if configured to do so. "
  - + some specifics whether fast or slow paths
- Router Alert is under discussion as:
  - Already used by MLD
  - Mainly as a semi-control plane indication to process on slow path

draft-ietf-6man-mtu-option

- Using a hop-by-hop option to record and signal the path MTU
- Of course, depends whether HbH are processed



```
 Option     Option     Option
  Type     Data Len    Data
+--------+--------+--------+--------+---------+-------+-+
|BBCTTTTT|00000100|     Min-PMTU     |     Rtn-PMTU     |R|
+--------+--------+--------+--------+---------+-------+-+

  Option Type (see Section 4.2 of [RFC8200]):

  BB      00   Skip over this option and continue processing.

  C        1   Option data can change en route to the packet's final
               destination.

  TTTTT 10000 Option Type assigned from IANA [IANA-HBH].
```

draft-ietf-6man-enhanced-vpn-vtn-id

- Carry some slice/VPN/... ID in a hop-by-hop option

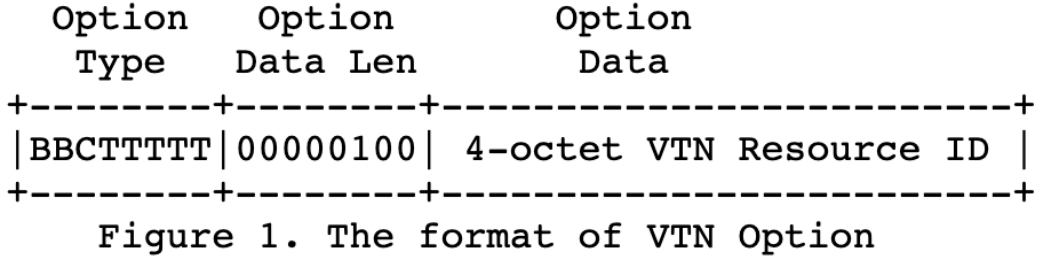


Figure 1. The format of VTN Option

- BBC == b000 == skip if not supported, no change on path
- Éric's issues:
  - Why scope if 5G slices only ?
  - Why a fixed length of 32 bit ?
  - Should there be flexibility to apply semantics in the ID ?

Thank you

- For listening
- But also, to ACT

- IETF is not about superpower of Gods
- It is about engineering mainly (and vendor politics sometime)
- Decisions are made on MAILING LIST
- Free
- You are an individual and not an employee/student
- No NEED to be in physical meetings