# IPv6 Extension Headers and Testing Results

Presented by: Nalini Elkins

NALINI ELKINS

INDUSTRY NETWORK TECHNOLOGY COUNCIL

PRESIDENT@INDUSTRYNETCOUNCIL.ORG

DHRUV DHODY

INDIA INTERNET ENGINEERING SOCIETY

INFO@IIESOC.IN

### Vision

Multi-year project: IPv6 deployment at enterprises.

Provide training,

Analysis of security and application conversion,

 Help enterprises plan their IPv6 deployment. India Internet Engineering Society (IIESoc) and Industry Network Technology Council (INTC)

#### **Grants: ISIF Asia**

- India Internet Engineering Society (IIESoc) and Industry Network Technology Council (INTC)
- Funding: Grant from ISIF Asia (https://isif.asia/2021-isif-as ia-grant-recipients-announc ed/#IPv6-webinar)
- Thank you!

https://www.iiesoc.in/



https://industrynetcouncil.org/

#### There is funding available to deploy IPv6





**2021 Funding Opportunities** 

**IPv6 Deployment Grants** 

For small and mid-size network operators in developing economies or large operators in underserved or remote areas.

# USD 800k in total

Available for funding requests from USD 30k - 250k

#### Find out more: www.isif.asia



#### **IPv6 Deployment Grants**



#### You need:

-An IPv6 allocation -To be in the Asia Pacific -A plan to deploy IPv6

#### You can get:

-USD 30,000 to 250,000 to help roll out IPv6 (minimum size is 30,000) Private companies, NGOs, universities, all kinds of organizations can apply.





# A few words about me

- President: Industry Network Technology Council
- Founder & CEO: Inside Products, Inc.
- Advisory Board: India Internet Engineering Society
- RFCs: RFC8250 (Embedded performance and diagnostics for IPv6) and others
- Product developer (OEMed by IBM and others)
- Working with IPv6 for 15 years
- Working with network management, diagnostic, performance issues at large brick-and-mortar enterprises for over 30 years



# Agenda

- IPv6 address structure
- IPv6 extension headers
  - Hop-by-hop
  - Fragment
  - Routing header
  - Destination Options header
  - IPSec
  - AH / ESP headers
- Issues

## IPv4 and IPv6 Headers

IPv4 Main Header (20 Bytes)					
Version	/ersion HdrLen Type of Service Total Length				
Identifica	ition		Flags Fragment Offset		
TimeToLive Protocol Checksum					
Source I	P Address	(4 bytes)			
Destination IP Address (4 bytes)					

IPv6 Main Header (40 Bytes)							
Version	/ersion Traffic Class Flow Label						
Payload I	Length		Next Header	Hop Limit			
Source Address (16 bytes )							
Destination Address (16 bytes)							

•What is the same?

#### •What is different?

# The IPv6 Header

- •IPv6 main header: fixed 40 bytes
- Source and destination addresses larger!
- Defined in RFC8200 (originally RFC2460)

#### IPv6 Main Header (40 Bytes)

Version	Traffic Class	Flow Label				
Payload	Length	Next Hdr Hop Limit				
Source A	Source Address					
Destination Address						

## **IP Header Structures**

- •Why IPv4 IPv6 headers so different?
- •Large IPv6 addresses!
- •Creation of extension headers

IPv4 Header : 20+ bytes

Source Address: 4 bytes

Dest. Address: 4 bytes

IPv4 Header + IPv6 address

Source Address: 16 bytes

Dest. Address: 16 bytes

Could become 44 bytes!

# **IPv6 Extension Headers**

- •New: IPv6 extension headers
- Next Header field chains headers
- •Rules:
  - May appear only once
  - Must appear in fixed order
  - •Exception: Destination Options

IPv6 Main Header (40 Bytes) Extension Header # 1 (next 5) Extension Header # 5 (next 8) Extension Header # 8 (next Data) Data

### Last IPv6 Extension Header

- •Last or only *Next Header* value
- •IPv4 Protocol field

Values in Next Header

Next Header (Decimal)	Header Name
1	ICMPv4
2	IGMPv4
4	IP in IP
6	TCP
17	UDP
41	IPv6
58	ICMPv6

## IPv6 Next Header Example

- Header chaining
- •Main extension header - payload

IPv6 Main Header (next 0)

Hop-by-Hop # 0 (next 44)

Fragment # 44 (next 6)

TCP Payload (Protocol 6)

# **Common IPv6 Extension Headers**

Next Header (Hex)	Next Header (Decimal)	Header Name	Description
0	0	Hop-by-Hop Options	For all devices on the path
2B	43	Routing	0 – Source Routing (deprecated) 2 – Mobile IPv6
2C	44	Fragment	Only when packet is fragmented
32	50	Encapsulated Security Payload (ESP)	IPSec encrypted data
33	51	Authentication Header (AH)	IPSec authentication
3C	60	Destination Options	http://www.iana.org/assignments /ipv6-parameters/ipv6-parameter s.xml (Mobile IP, etc)

No	o. 🗸 Time	Source	Destination	Pro
	1693 46.130640		ff02::2	IC
Ŧ	Frame 1693 (86 by	ytes on wire, 86 b	ytes captured)	Det 1
2	Destination: IF Source: 192.168	Pv6-Neighbor-Disco 3.1.1 (00:14:bf:ba	very_00:00:00:02 :45:f9)	(33:33
	Type: IPv6 (0x8	36dd)		
-	Internet Protoco	l Version 6		
	Version: 6	0.000		
	Traffic class:	0×00		
	Flowlabel: 0x00	2000		
	Payload length:	: 32		
	Next header: IF	∿% hop-by-hop opt	10n (0x00)	
	Hop Inmit: 1			
	Source address:	: ::		
	Destination add	aress: TT02::2		
-	Hop-by-hop option	n Header		
	Next header: 10	IMPV6 (UX3a)		
	Length: U (8 b)	/tesj		
	Router alert: M	ILD (4 bytes)		
	PadN: 2 bytes	Manager Dustage]		
=	Thernet Control	Message Protocol	VO	
	Code: 0	licast listener re	portj	
	Checksum: 0x7ea	13 [correct]		
	Maximum respons	se delay: O		
	Multicast Addre	ess: ff02::2		

# IPv6 Hop-by-Hop Header

Size (bits)	Field Name	Description
8	Next Header	Contains the protocol number of the next header
8	Length	Length of this header in octets (bytes)
Variable	Options	8 bits for type, length in bytes, and then the option itself <u>http://www.iana.org/assignments/ipv6-parameters/ipv6-p</u> <u>arameters.xml</u>

Remember: this has to be read by every device!

# Sample Fragment Header

lo.		Time	Source	Destination
	5762	80.385670	2001:4998:0:6::15	2607:f740:0:3f:216:3eff:fe68:72c0
•				
÷	Frame	5762: 1494 b	ytes on wire (11952 b	oits), 1494 bytes captured (11952 bits)
+	Etherr	net II, Src:	Cisco_ae:30:0a (00:00	::cf:ae:30:0a), Dst: Xensourc_68:72:c0 (
-	Interr	net Protocol	version 6, Src: 2001:	:4998:0:6::15 (2001:4998:0:6::15), Dst:
	⊕ 0110	) = Vers	ion: 6	
	±	0000 0000 .		= Traffic class: 0x00000000
		0	101 0100 0001 0000 11	LOO = Flowlabel: 0x0005410c
	Pay	load length: :	1440	
	Next	: header: IPv	6 fragment (0x2c)	
	нор	limit: 56	55	
	Sour	ce: 2001:499	8:0:6::15 (2001:4998:	:0:6::15)
	Dest	ination: 260	7:f740:0:3f:216:3eff:	:fe68:72c0 (2607:f740:0:3f:216:3eff:fe68
	[Des	stination SA	MAC: Xensourc_68:72:0	:0 (00:16:3e:68:72:c0)]
	🗆 Fraç	gmentation He	ader	
	Ne	ext header: T	CP (0x06)	
	00	0000 0000 0000	0 = Offset: 0 (0)	<0000)
			1 = More Fragment	:: Yes
	IC	dentification	: 0xa262a3bc	
	Reas	sembled IPv6	in frame: 5763	
+	Data (	(1432 bytes)		

# IPv6 Fragment Header

Size (bits)	Field Name	Description
8	Next Header	Points to next header or payload
8	Reserved	Set to 0.
13	Fragment Offset	Points to where in original packet this fragment goes (units of 8 bytes)
2	Reserved	Set to 0.
1	M Flag	More fragments to come or not
32	Identification	Identify all fragments in same packet

Remember: Fragmentation is not supported at routers. It is only supported at the originating host.

## **IPv6** Destination Options

### •Destination Options: for end host



## **IPv6** Destination Options

```
∃ Frame 1: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits)
Prism capture header
∃ IEEE 802.11 Data, Flags: .....T
E Logical-Link Control
Internet Protocol Version 6, Src: 2001:720:810:1212:209:b7ff:fe3c:902c (2001:720:810:1212:209:b7

    ⊕ 0110 .... = Version: 6

 ⊞ .... 0000 0000 .... ... ... ... = Traffic class: 0x00000000
   .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
   Payload length: 40
   Next header: IPv6 destination option (60)
   Hop limit: 255
   Source: 2001:720:810:1212:209:b7ff:fe3c:902c (2001:720:810:1212:209:b7ff:fe3c:902c)
   [Source SA MAC: Cisco_3c:90:2c (00:09:b7:3c:90:2c)]
   Destination: 2001:720:810:1213::1 (2001:720:810:1213::1)
   [Source GeoIP: Unknown]
   [Destination GeoIP: Unknown]
                                                            Use of Destination
 Destination Option
    Next header: Mobile IPv6 (62)
                                                          Options in Mobile IPv6
    Length: 2 (24 bytes)
   □ IPv6 Option (PadN)
      Type: PadN (1)
      Length: 2
      PadN: 0000
   □ IPv6 Option (Home Address)
      Type: Home Address (201)
      Length: 16
      Home Address: 2001:720:810:1213::2 (2001:720:810:1213::2)
∃ Mobile IPv6 / Network Mobility
```

```
Vo.
      Time
                                                            Destination
                              Source
                               3001::200:10ff:fe10:1181
                                                            3000::200:10ff:fe10:1060
    1 0.000000
4
                                                                         111
Frame 1: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
Ethernet II, Src: Hughes_10:10:60 (00:00:10:10:60), Dst: IntelCor_16:c7:fe (00:15:17:16:c7)
Internet Protocol Version 6, Src: 3001::200:10ff:fe10:1181 (3001::200:10ff:fe10:1181), Dst: 3

    ⊕ 0110 .... = Version: 6

 .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
   Payload length: 65
   Next header: IPv6 routing (43)
   Hop limit: 255
   Source: 3001::200:10ff:fe10:1181 (3001::200:10ff:fe10:1181)
   [Source SA MAC: Hughes_10:11:81 (00:00:10:10:11:81)]
   Destination: 3000::215:17ff:fe16:c7fe (3000::215:17ff:fe16:c7fe)
   [Destination SA MAC: IntelCor_16:c7:fe (00:15:17:16:c7:fe)]
   [Source GeoIP: Unknown]
   [Destination GeoIP: Unknown]
 □ Routing Header, Type : IPv6 Source Routing (0)
     Next header: ICMPv6 (58)
     Length: 6 (56 bytes)
     Type: IPv6 Source Routing (0)
     Segments Left: 1
     Address: 3002::200:10ff:fe10:1262 (3002::200:10ff:fe10:1262)
     Address: 3003::200:10ff:fe10:1363 (3003::200:10ff:fe10:1363)
     Address: 3000::200:10ff:fe10:1060 (3000::200:10ff:fe10:1060)
Internet Control Message Protocol v6
   Type: Echo (ping) request (128)
   Code: 0
 E Checksum: 0x1d00 [incorrect, should be 0xdbb9]
   [Bad Checksum: True]
   Identifier: 0x0000
   Sequence: 0
 Data (1 byte)
```

# RFC5095 (Deprecation of Type 0 Routing Headers in IPv6)

- RHO : can create routing loops.
- Deprecated
- Segments Left = zero, ignore
- Segments Left > zero, send
   ICMPv6 error message



No		Time	Source	Destination	Protocol	Info
	24 25 26 27 28 29 30 31	22.033413 22.033498 22.033683 22.034033 22.035602 22.037826 22.061508 22.061630	192.168.1.102 192.168.1.101 192.168.1.102 192.168.1.102 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101 192.168.1.101	192.168.1.101 192.168.1.102 192.168.1.101 192.168.1.101 192.168.1.102 192.168.1.102 192.168.1.101 192.168.1.102 192.168.1.102	ESP ESP ESP ESP ESP ESP ESP	ESP (SPI=0x721d6491) ESP (SPI=0x84feb4c2) ESP (SPI=0x721d6491) ESP (SPI=0x721d6491) ESP (SPI=0x84feb4c2) ESP (SPI=0x721d6491) ESP (SPI=0x84feb4c2) ESP (SPI=0x84feb4c2)
±	Frame Ether Inter	e 24 (94 byt net II, Src net Protoco	es on wire, 94 byte : 192.168.1.102 (00 ]. src: 192.168.1.1	es captured) ):13:d3:8d:61:fb), D LO2 (192.168.1.102).	st: 19 Dst:	2.168.1.101 (00:11:d8:39:29:2b) 192.168.1.101 (192.168.1.101)
	Ver Hea Tot Ide Fla Fra Tim Pro Hea Sou Des	sion: 4 der length: ferentiated al Length: entification gs: 0x04 (D gment offse to live: tocol: ESP der checksu rce: 192.16 tination: 1	20 bytes Services Field: 0> 80 : 0x0e40 (3648) on't Fragment) t: 0 128 (0x32) m: 0x6820 [correct] 8.1.102 (192.168.1. 92.168.1.101 (192.1	<pre>&lt;00 (DSCP 0x00: Defa 102) .68.1.101)</pre>	ult; E	CN: 0×00) Notice the IP Header and then the ESP (Encapsulating Security Payload) Header
=	SPI Sec	: 0x721d649 uence: 1	1			
	Dat	a (Jz bytes				

No	Time	Source	Destination	Protocol	Info
	54 58.975378	192.168.1.102	192.168.1.101	ICMP	Echo (ping) request
	ame 54 (98 byt hernet II, Src	es on wire, 98 byte : 192.168.1.102 (00 ] src: 192.168.1 1	s captured) :13:d3:8d:61:fb), Ds 02 (192 168 1 102)	st: 192	.168.1.101 (00:11:d8:39:29:2b) 92 168 1 101 (192 168 1 101)
⊡ Int ∨ ⊢ ⊡ C I I F F	Version: 4 Header length: Differentiated Total Length: S Contification Tags: 0x00	7, 3rC. 192.108.1.1 20 bytes Services Field: 0x 84 : 0xcf62 (53090)	02 (192.108.1.102), 00 (DSCP 0x00: Defau	ult; ECI	n: 0x00)
F T E E C	ragment offse ime to live: : rotocol: AH ( leader checksur Source: 192.16 estination: 1	t: 0 128 0x33) m: 0xe6f8 [correct] 8.1.102 (192.168.1.) 92.168.1.101 (192.1	102)	• No en	otice the data itself is not crypted.
E Aut N L S I	Hentication H Next Header: Io Length: 24 SPI: 0xe64fdf2 Sequence: 1	eader CMP (0x01)		typ lev im	be is ICMP. Any higher vel protocol may be bedded.
🗏 Int	ernet Control	Message Protocol			
	ype: 8 (Echo Code: 0 Checksum: 0x05 Cdentifier: 0x0 Sequence number Data (32 bytes)	(ping) request) 5b [correct] 0200 r: 0x4601 )			
0000 0010 0020 0030 0040 0050 0060	00 11 d8 39 2 00 54 cf 62 0 01 65 01 04 0 9d 3d 4b 55 k 46 01 61 62 6 6f 70 71 72 7 68 69	29 2b 00 13 d3 8d 0 00 00 80 33 e6 f8 0 00 00 e6 4f df 2c 0 09 f8 48 4b 1f a0 0 63 64 65 66 67 68 0 73 74 75 76 77 61 0	51 fb 08 00 45 00 50 a8 01 66 c0 a8 50 00 00 01 67 5f 58 00 05 5b 02 00 59 6a 6b 6c 6d 6e 52 63 64 65 66 67	9)+. .T.b .e .=KUF F.abcde opgrstu hi	E. .3f. .0 .,g_ HK[ ef ghijklmn uv wabcdefg

Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) Ethernet II, Src: c2:00:68:b3:00:01 (c2:00:68:b3:00:01), Dst: IPv6mcast\_00: Destination: IPv6mcast\_00:00:00:05 (33:33:00:00:05) E Source: c2:00:68:b3:00:01 (c2:00:68:b3:00:01) Type: IPv6 (0x86dd) Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::5 (ff02::5) ⊕ 0110 .... = Version: 6
 .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000 Payload length: 60 Next header: AH (51) Hop limit: 1 IPv6 Packet with AH only. Source: fe80::1 (fe80::1) Destination: ff02::5 (ff02::5) Notice that this is an [Source GeoIP: Unknown] **OSPF** packet! [Destination GeoIP: Unknown] So we can have many Authentication Header Next Header: OSPF IGP (0x59) protocols protected. Length: 24 AH SPI: 0x00000100 AH Sequence: 19 AH ICV: 21d3a95c5ffd4d184622b9f8 Open Shortest Path First OSPE Header OSPE Version: 3 Message Type: Hello Packet (1) Packet Length: 36 Source OSPF Router: 1.1.1.1 (1.1.1.1) Area ID: 0.0.0.1 Packet Checksum: 0xfb86 [correct] Instance ID: 0 (IPv6 unicast AF)

# **Authentication Header**

- Integrity: hash algorithms (ex. MD5 or SHA)
- The inputs to the hash algorithm are:
  - a secret key,
  - the payload of the packet, and
  - the unchangeable parts of the IP header, like the IP addresses.
- Source authentication: secret key
- Replay protection (optional): sequence numbers
- No encryption

- A hash function is a computation that takes a variable-size input and returns a fixed-size string, which is called the hash value.
- If the hash function is one-way (that means hard to invert), it is also called a message-digest function.
- It is a digital fingerprint of the larger document.



# **ESP Header**

- •ESP = Encapsulating Security Payload
- •AH 'lighter' authentication
- Standard symmetric encryption algorithms (3DES, AES, Blowfish, etc)
- IP Packet IP Header ESP : HMAC (xxxx) TCP, UDP, ICMP, IP With ESP, the upper level protocol data is encrypted using the chosen algorithm.
- •Encryption 🛛 hash 🖓 generate ESP header

#### Issues

- •Routers may drop
- •Extension headers may be too big (ASIC size)
- Privacy violations
- •Change the extension header not at source
- Parsing of TLV (Type, length, value)

# Pros

- •New protocol functions = extensible protocol, long maturity
- •PDM / PDMv2 : embedded performance and diagnostic metrics + encryption methodology for IPv6 extension headers (RFC8250, et al)
- •Many others: source address validation

# Malformed Packets

#### Manipulate headers

- •IPv6 incorrect or partial header
- •Violate header order
- •Violate header option restrictions

IPv6 Main Header (40 Bytes)							
Version Traffic Class Flow Label							
Payload I	Payload Length Next Hdr Hop Limit						
Source Address							
Destination Address							

```
No.
       Time
                               Source
                                                  Destination
                                                                    Protocol
     1 0.000000
                               2a01:e35:8bd9:8bb0:2001:4b98:dc0:41:21 UDP
     2 0.050763
                               2001:4b98:dc0:41:212a01:e35:8bd9:8bb0:ICMPv6
Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
Ethernet II, Src: AsustekC_76:29:b6 (00:1e:8c:76:29:b6), Dst: FreeboxS_4d:1f:41 (f4)
Internet Protocol Version 6, Src: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35)

    ⊕ 0110 .... = Version: 6

  .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 26
    Next header: IPv6 destination option (60)
    Hop limit: 64
    Source: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8
    Destination: 2001:4b98:dc0:41:216:3eff:fece:1902 (2001:4b98:dc0:41:216:3eff:fece
    [Destination 5A MAC: Xensourc_ce:19:02 (00:16:3e:ce:19:02)]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
                                        From RFC2460: Option 11: discard the
  Destination Option
                                        packet and, only if the packet's Destination
      Next header: UDP (17)
      Length: 0 (8 bytes)
                                        Address was not a multicast address, send
    □ IPv6 Option (Unknown 11)
                                        an ICMP Parameter Problem, Code 2,
        Type: Unknown (11)
                                        message to the packet's Source Address,
        Length: 1
        Unknown Option Payload: 09
                                        pointing to the unrecognized Option Type.
    □ IPv6 Option (PadN)
        Type: PadN (1)
        Length: 1
        PadN: 00
User Datagram Protocol, Src Port: 42513 (42513), Dst Port: name (42)
    Source port: 42513 (42513)
```

#### **Crafted Packet**



Crafted IPv6 packet

•Multiple headers

Deprecated headers

# •Headers out of order

# Can IPv6 Extension Headers Be Used on the Internet?

- Controversy for many years
- A number of studies showing that IPv6 extension headers "don't work"
- Studies (by and large) sent "fake" IPv6 extension headers to Alexa top n sites
- If this is true, our work on our IPv6 Extension Header Destination Option Performance and Diagnostic Metrics (PDM) is really for naught

#### Brief explanation of PDM

- RFC8250: IPv6 Performance and Diagnostic Metrics (PDM) Destination Option
- To assess performance problems, this document describes optional headers embedded in each packet that provide sequence numbers and timing information as a basis for measurements. Such measurements may be interpreted in real time or after the fact. This document specifies the Performance and Diagnostic Metrics (PDM) Destination Options header.

#### What we did

- Used a small hosting service (not one of the "brand-name" ones)
- Locations throughout the world
- 1. PDM-Warsaw
- 2. PDM-Toronto
- 3. PDM-Seattle
- 4. PDM-Mumbai
- 5. PDM-Melbourne
- 6. PDM-Frankfurt

All machines are FreeBSD with a modification to the kernel to send PDM IPv6 Destination option with every packet

#### Thanks to ...





Industry Network Technology Council

# Tested large FTP: Toronto to Mumbai (with PDM)

- Connected to 2401:c080:2400:1179:5400:04ff:fe0f:804a.
- 220------ Welcome to Pure-FTPd [privsep] [TLS] ------
- 220-You are user number 1 of 50 allowed.
- 220-Local time is now 15:12. Server port: 21.
- 220 You will be disconnected after 15 minutes of inactivity.
- 331 User PDMuser OK. Password required
- 230 OK. Current directory is /
- Remote system type is UNIX.
- Using binary mode to transfer files.

- 229 Extended Passive mode OK (|||3353|)
- 150-Accepted data connection
- 150 27872.0 kbytes to download
- 226-File successfully transferred
- 226 125.107 seconds (measured here), 222.78 Kbytes per second
- 28540928 bytes received in 02:05 (222.31 KiB/s)
- 221-Goodbye. You uploaded 0 and downloaded 27872 kbytes.
- 221 Logout.

#### **Trace of Extension Headers**

#### FTPTorontoToMumbaiJustIPv6.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

📶 🔳 🖉 📵 📕 🖺 🕱 🗳 🧣 🔿 🖉 🖌 📜 🔍 Q, Q, 🎹

Apply a display filter ... <Ctrl-/>

From PDM IPv6 DOH

Vo.	Time	Source	Destination	Protocol	PSN This Packet PSN Last R	Received Info	
	38 2.857775	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	TCP	20489	0 61272 → 53696 [SYN] Seq=0 Win=65535 Len=0 M	
	39 2.963460	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	TCP	14104	12376 62443 → 21 [ACK] Seq=101 Ack=805 Win=66240	1
1. 12	40 3.056635	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	ТСР	23911	20489 53696 → 61272 [SYN, ACK] Seq=0 Ack=1 Win=65	Ī
1	41 3.056686	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	TCP	20490	23911 61272 → 53696 [ACK] Seq=1 Ack=1 Win=66240 L	
	42 3.056735	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	FTP	14105	12376 Request: RETR out.txt	-
	43 3.253255	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=0 more=y ident=0x73059a8-	-
10	44 3.253284	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=1432 more=y ident=0x7305	
	45 3.253290	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=2864 more=y ident=0x7305	
33	46 3.253298	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=4296 more=y ident=0x7305	
	47 3.253304	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=5728 more=y ident=0x7305	
23	48 3.253315	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=7160 more=y ident=0x7305	
1	49 3.253326	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=8592 more=y ident=0x7305	
	50 3.253332	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=10024 more=y ident=0x730	
	51 3.253341	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23912	20490 IPv6 fragment (off=11456 more=y ident=0x730	
1	52 3.253350	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	FTP-DATA	23912	20490 FTP Data: 14280 bytes (EPASV) (RETR out.txt	
	53 3.253399	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	TCP	20491	23912 61272 → 53696 [ACK] Seq=1 Ack=14281 Win=519	
	54 3.266651	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	FTP	12377	14105 Response: 150-Accepted data connection	
	55 3.372449	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	ТСР	14106	12377 62443 → 21 [ACK] Seq=115 Ack=867 Win=66240	
	56 3.449235	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=0 more=y ident=0x7acf3f8	
	57 3.449249	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=1432 more=y ident=0x7acf	
	58 3.449277	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=2864 more=y ident=0x7acf	
	59 3.449283	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=4296 more=y ident=0x7acf	2
	60 3.449289	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=5728 more=y ident=0x7acf	
0	61 3.449316	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=7160 more=y ident=0x7acf	
	62 3.449324	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=8592 more=y ident=0x7acf	
	63 3.449336	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=10024 more=y ident=0x7ac	
	64 3.449349	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=11456 more=y ident=0x7ac	
0	65 3.449355	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=12888 more=y ident=0x7ac	
	66 3.449363	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	IPv6	23913	20491 IPv6 fragment (off=14320 more=y ident=0x7ac	
	67 3.449369	2401:c080:2400:1179:5400:4ff:fe0f:804a	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	FTP-DATA	23913	20491 FTP Data: 17136 bytes (EPASV) (RETR out.txt	
	68 3.449430	2001:19f0:b001:6ce:5400:4ff:fe0f:806d	2401:c080:2400:1179:5400:4ff:fe0f:804a	TCP	20492	23913 61272 → 53696 [ACK] Seq=1 Ack=31417 Win=490	

>

Х

#### Showing both Extension Headers



#### **Bottom line**

- 1. PDM-FTP Toronto to Warsaw worked
- 2. PDM-FTP Toronto to Seattle worked
- 3. PDM-FTP Toronto to Mumbai worked
- 4. PDM-FTP Toronto to Melbourne worked
- 5. PDM-FTP Toronto to Frankfurt worked

Traces available for all to look at.

Come to the Hackathon (or HackDemo) if you want to see for yourself.

#### PDMv2 for Monitoring Encrypted Traffic



#### IAB workshop on Management Techniques in Encrypted Networks (M-TEN), 2022

Home»Activities»Workshops»IAB workshop on Management Techniques in Encrypted Networks (M-TEN), 2022

User privacy and security are constantly being improved by increasingly strong and more widely deployed encryption. This workshop aims to discuss ways to improve network management techniques in support of even broader adoption of encryption on the Internet.

#### Our proposal was accepted!

#### Next steps ...

- •Test with:
  - CDNs
  - •Cloud providers
  - •Routers
  - •ISPs
  - Load balancers
  - •OSs
- •Need to test ALL extension headers!
- •This will be a two-year process!



Contact:

#### info@iiesoc.in

#### president@industrynetcouncil.org

## IPv4 – IPv6 Protocol Differences

		IPv4	IPv6	
1.	Source and destination addresses are bits (4 bytes) in length.	e 32	1. Sourd bits (	ce and destination addresses are 128 16 bytes) in length
2.	Fragmentation is supported at origin hosts and at intermediate routers.	ating	2. Fragr It is o	nentation is not supported at routers. Inly supported at the originating host.
3.	IP header includes a checksum.		3. IP he	ader does not include a checksum.
4.	IP header includes options.		4. All or head	otional data is moved to IPv6 extension ers.
5.	IPsec support is not mandatory.		5. IPsec imple	support is required in a full IPv6 ementation.
6.	No identification of payload for QoS handling by routers is present within IPv4 header.	the	6. Paylo route the F	ad identification for QoS handling by ers is included in the IPv6 header using low Label field.
7.	In IPv4, the minimum MTU for route physical links is 576 bytes.	rs and	7. In IP\ MTU	6, all links must handle a minimum of at least 1280 bytes.

#### The IPv4 Header

Size (bits)	Field	Description
4	Version	4 : version of IP
4	Header Length	Length of header in Words (Word = 32 bits)
8	Type of Service (TOS)	Quality of Service : Differentiated Services Code Point (DSCP – RFC2474) and Explicit Congestion Notification (ECN - RFC3168)
16	Total Length	Total length of the entire packet. Max: 65,535
16	Identification	Identify all fragments in same packet. Max: 65,535
3	Flags	More fragments to come or not
13	Fragment Offset	Points to where in original packet this fragment goes (units of 8 bytes)
8	Time To Live	Hops (routers) to go to before dropping packet
1	Protocol	What kind of upper layer protocol or data is in this packet
2	Header Checksum	Integrity check on the header
32	Source Address	The sender of the packet
32	Destination Address	The receiver of the packet
-	Options + Padding	Variable length

### The IPv6 Header

Size (bits)	Field	Description
4	Version	6
8	Traffic Class	Quality of Service : Differentiated Services Code Point (DSCP – RFC2474) and Explicit Congestion Notification (ECN - RFC3168)
20	Flow Label	Quality of Service : real time (RFC2460 and many others!)
16	Payload Length	Bytes in the IPv6 extension headers and payload.
8	Next Header	Points to extension header or payload
8	Hop Limit	Hops (routers) to go to before dropping packet
128	Source Address	The sender of the packet
128	<b>Destination Address</b>	The receiver of the packet