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-asia-grant-recipients-announced/#IPv6-webinar)
- Thank you!

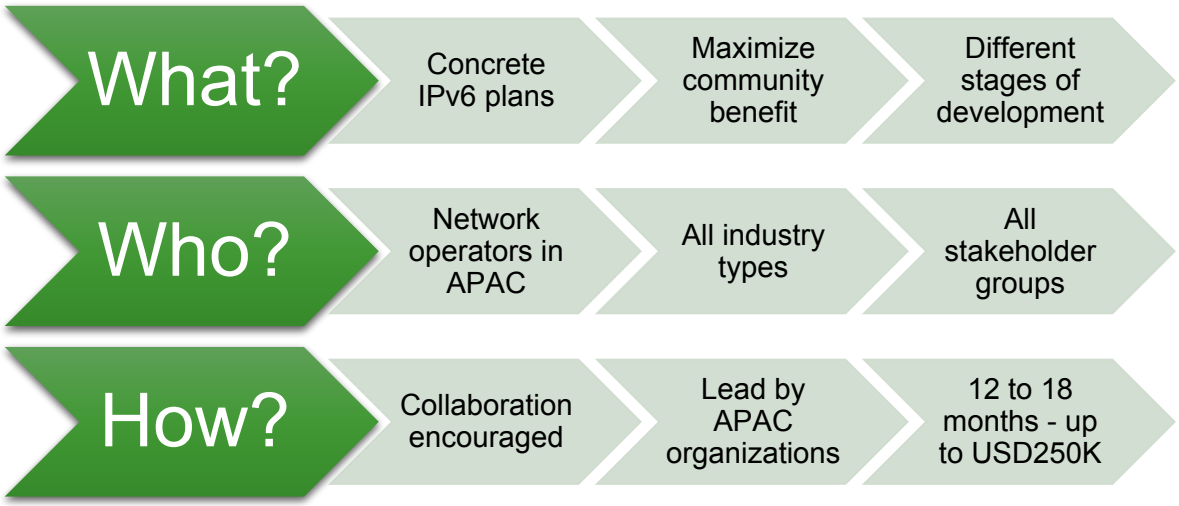
https://www.iiesoc.in/

https://industrynetcouncil.org/

There is funding available to deploy IPv6

APNIC FOUNDATION

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.

APNIC FOUNDATION

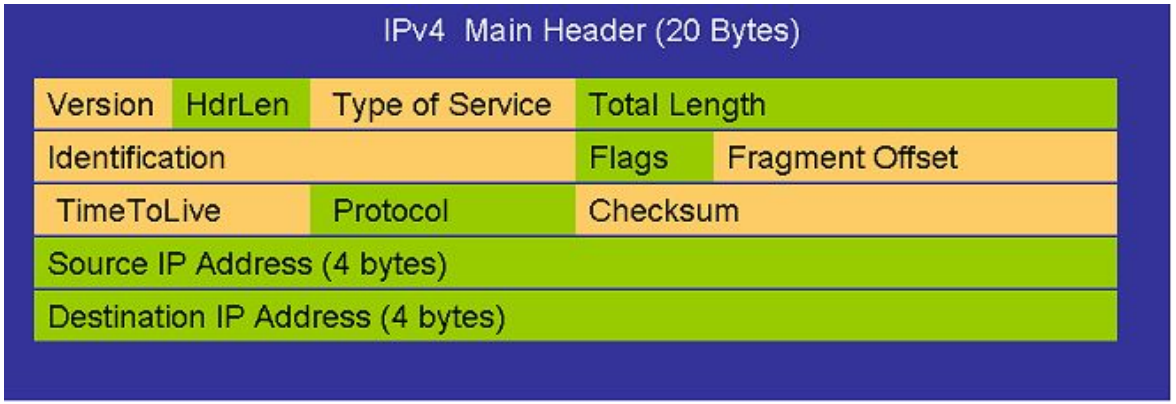
A few words about me

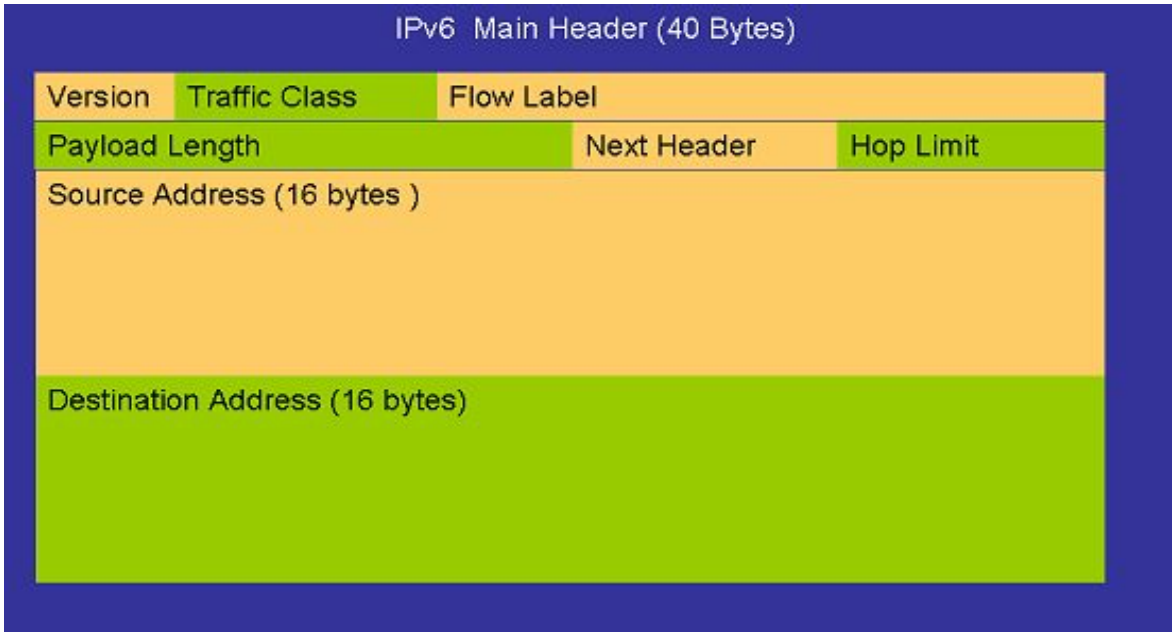
- President: Industry Network Technology Council
- Founder & CEO: Inside Products, Inc.
- Advisory Board: India Internet Engineering Society
- RFCs: RFC8250 (Embedded performance and diagnostics for IPv6) and others
- Product developer (OEMed by IBM and others)
- Working with IPv6 for 15 years
- Working 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

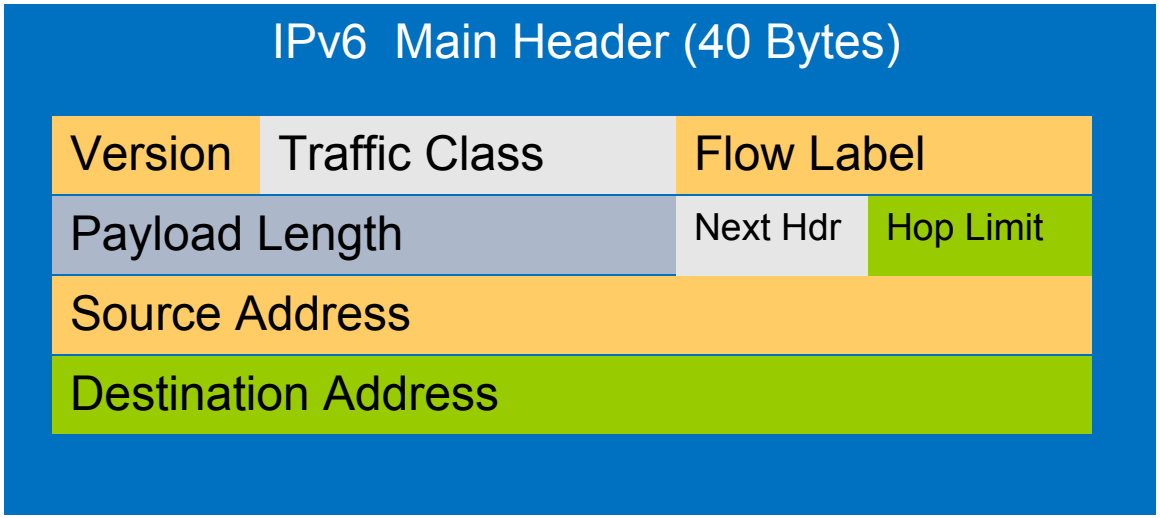




- What is the same?
- What is different?

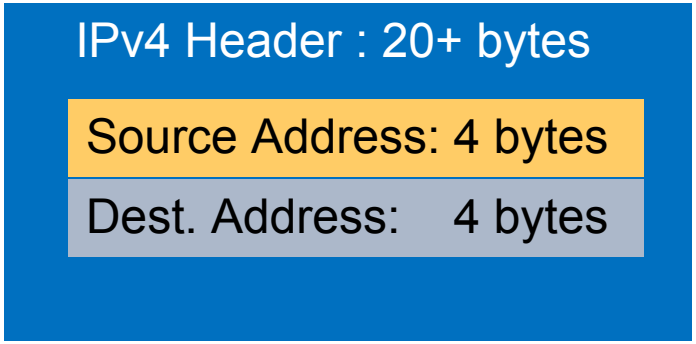
The IPv6 Header

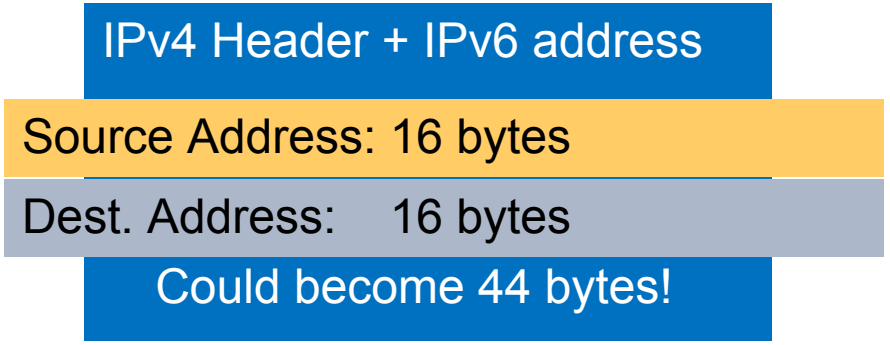
- IPv6 main header: fixed 40 bytes
- Source and destination addresses larger!
- Defined in RFC8200 (originally RFC2460)



IP Header Structures

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

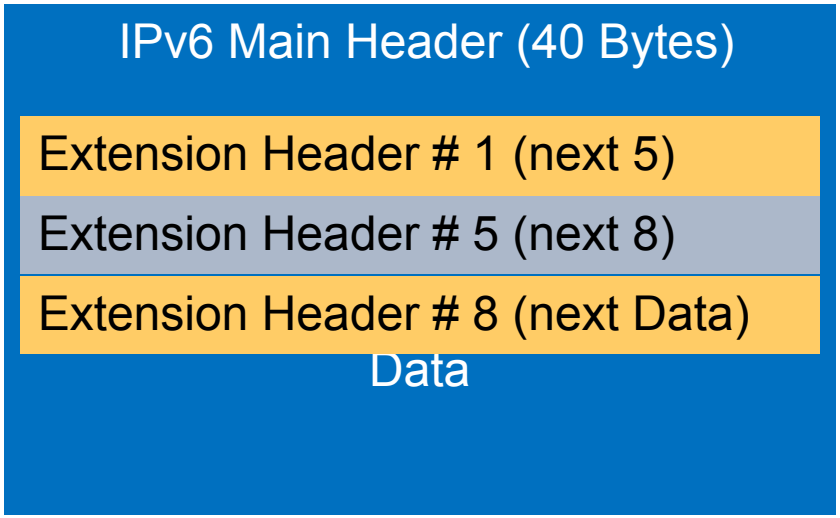




IPv6 Extension Headers

- New: IPv6 extension headers
- Next Header field chains headers

- Rules:
  - May appear only once
  - Must appear in fixed order
  - Exception: Destination Options



Last IPv6 Extension Header

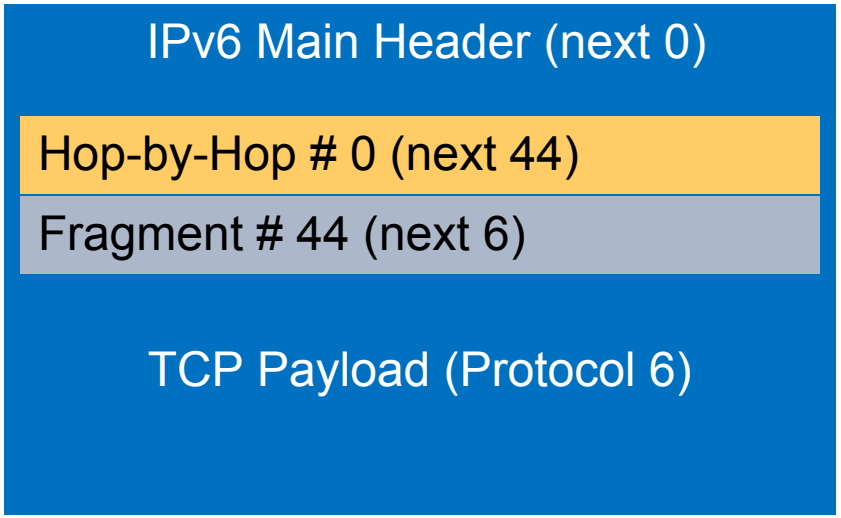
- Last or only *Next Header* value
- IPv4 *Protocol* field

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

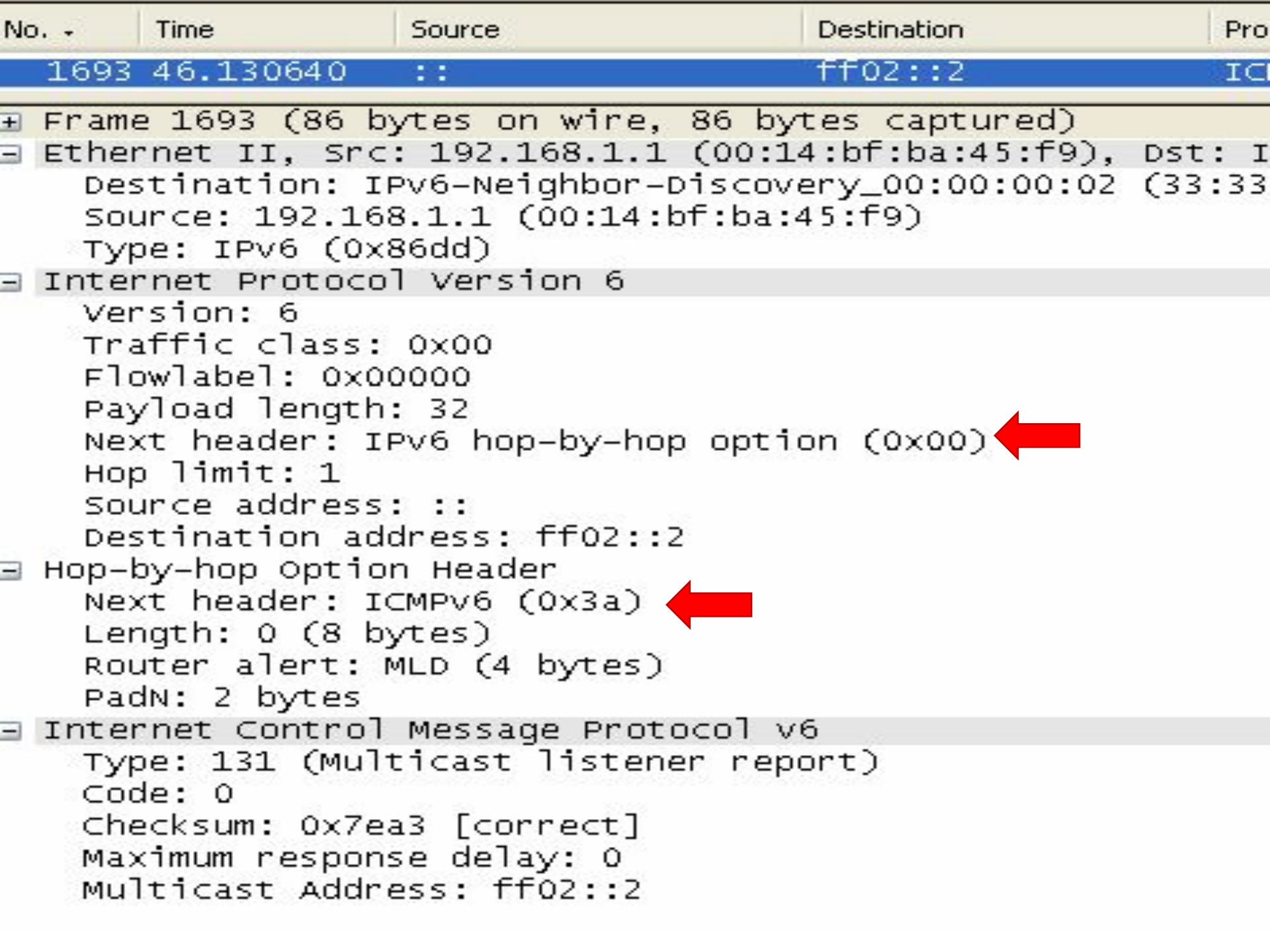
IPv6 Next Header Example

- Header chaining
- Main – extension header - payload



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-parameters.xml (Mobile IP, etc)

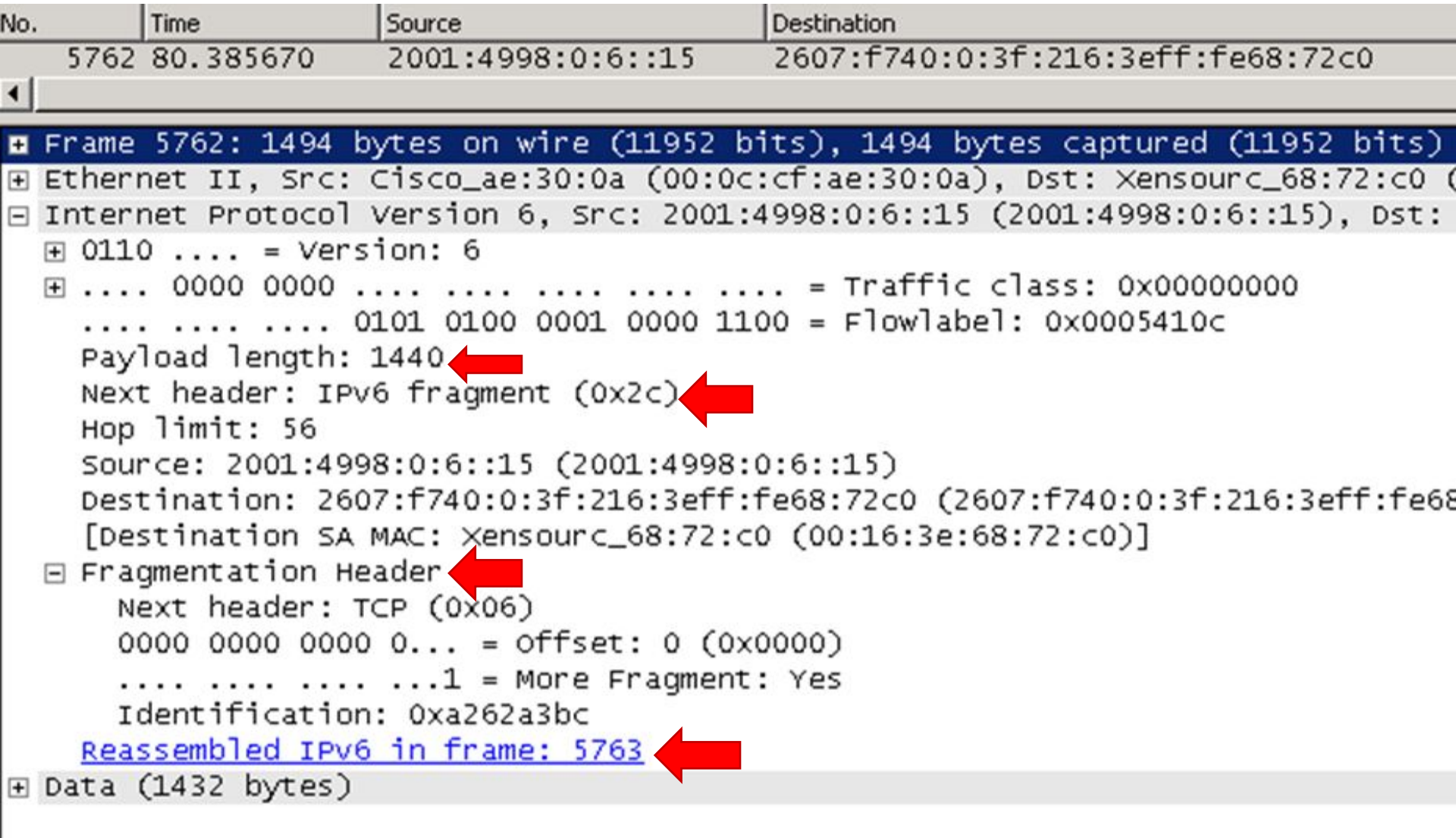

No. Time Source Destination Pro
1693 46.130640 :: ff02::2 IC
Frame 1693 (86 bytes on wire, 86 bytes captured)
Ethernet II, Src: 192.168.1.1 (00:14:bf:ba:45:f9), Dst: I
Destination: IPv6-Neighbor-Discovery_00:00:00:02 (33:33
Source: 192.168.1.1 (00:14:bf:ba:45:f9)
Type: IPv6 (0x86dd)
Internet Protocol Version 6
Version: 6
Traffic class: 0x00
Flowlabel: 0x00000
Payload length: 32
Next header: IPv6 hop-by-hop option (0x00)
Hop limit: 1
Source address: ::
Destination address: ff02::2
Hop-by-hop Option Header
Next header: ICMPv6 (0x3a)
Length: 0 (8 bytes)
Router alert: MLD (4 bytes)
PadN: 2 bytes
Internet Control Message Protocol v6
Type: 131 (Multicast listener report)
Code: 0
Checksum: 0x7ea3 [correct]
Maximum response delay: 0
Multicast Address: 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** http://www.iana.org/assignments/ipv6-parameters/ipv6-parameters.xml

Remember: this has to be read by every device!

Sample Fragment Header



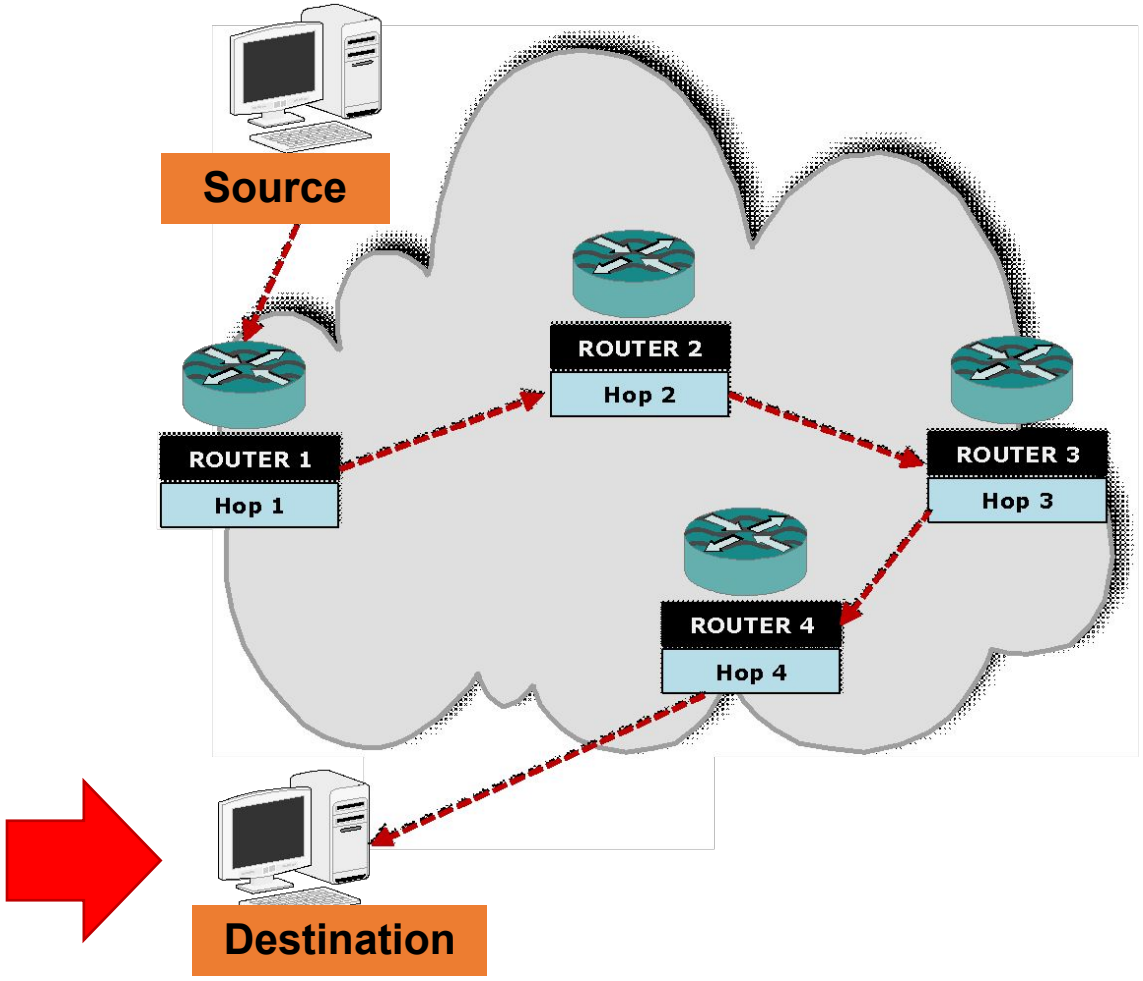
IPv6 Fragment Header

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

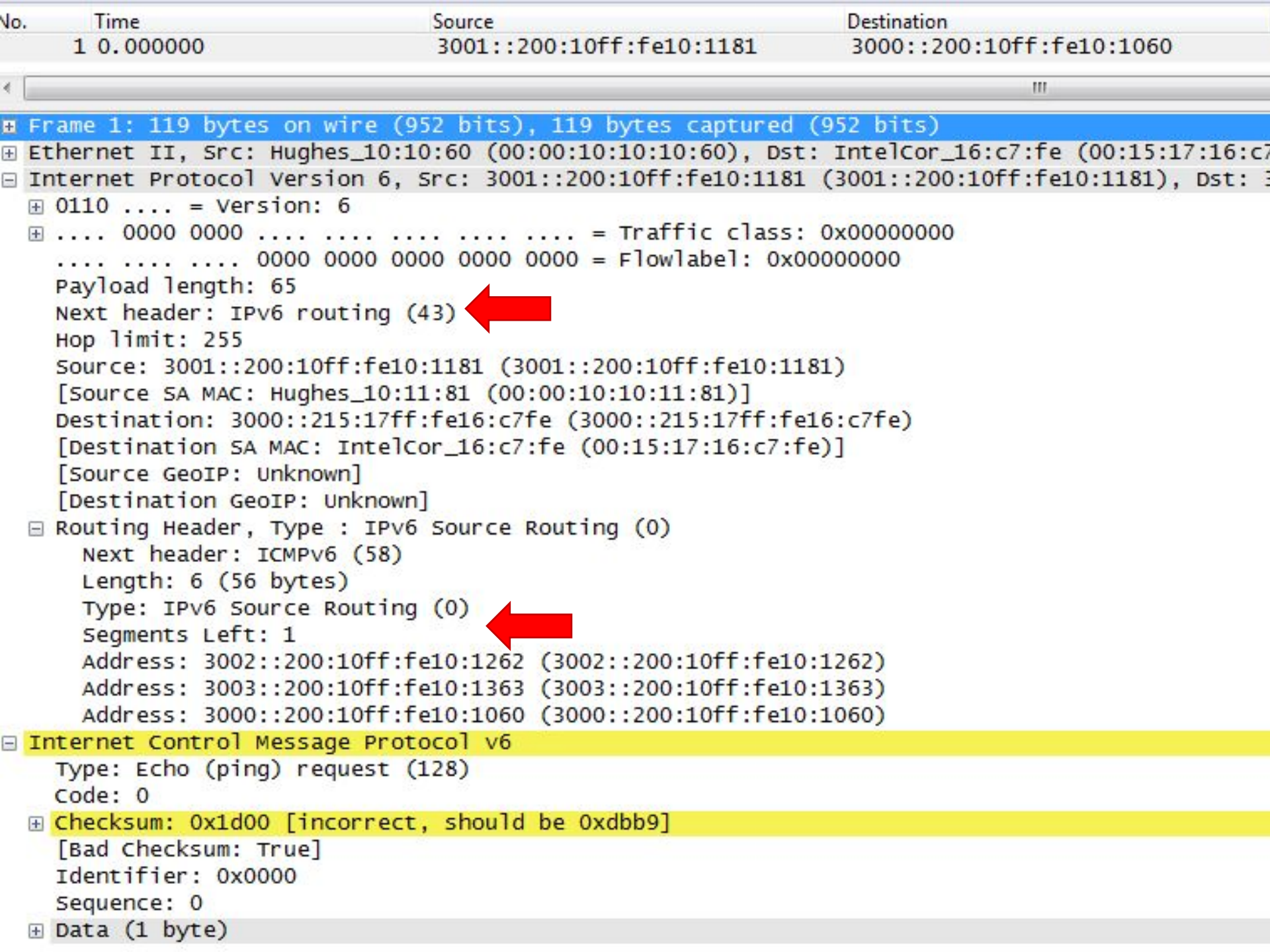
- Destination Options: for end host



IPv6 Destination Options

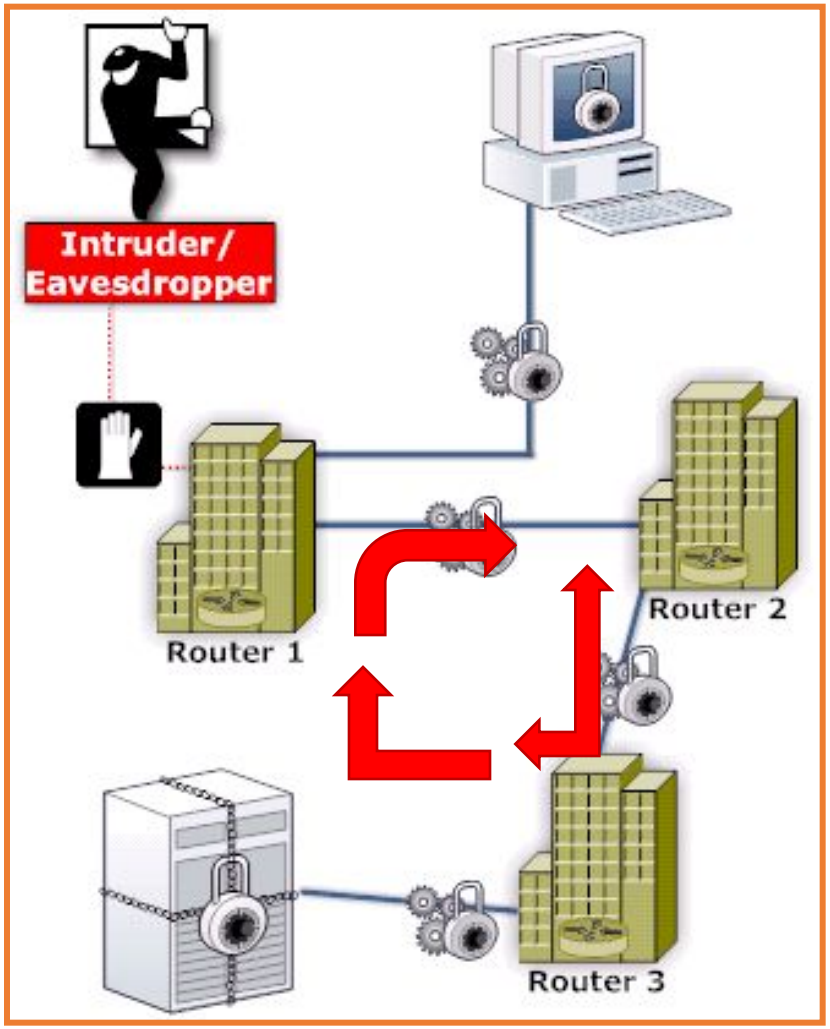
```
⊞ Frame 1: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits)
⊞ Prism capture header
⊞ IEEE 802.11 Data, Flags: .......T
⊞ Logical-Link Control
⊟ Internet Protocol Version 6, Src: 2001:720:810:1212:209:b7ff:fe3c:902c (2001:720:810:1212:209:b7
  ⊞ 0110 .... = Version: 6
  ⊞ .... 0000 0000 .... .... .... .... .... = 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]
  ⊟ Destination Option
      Next header: Mobile IPv6 (      (62)
      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
```

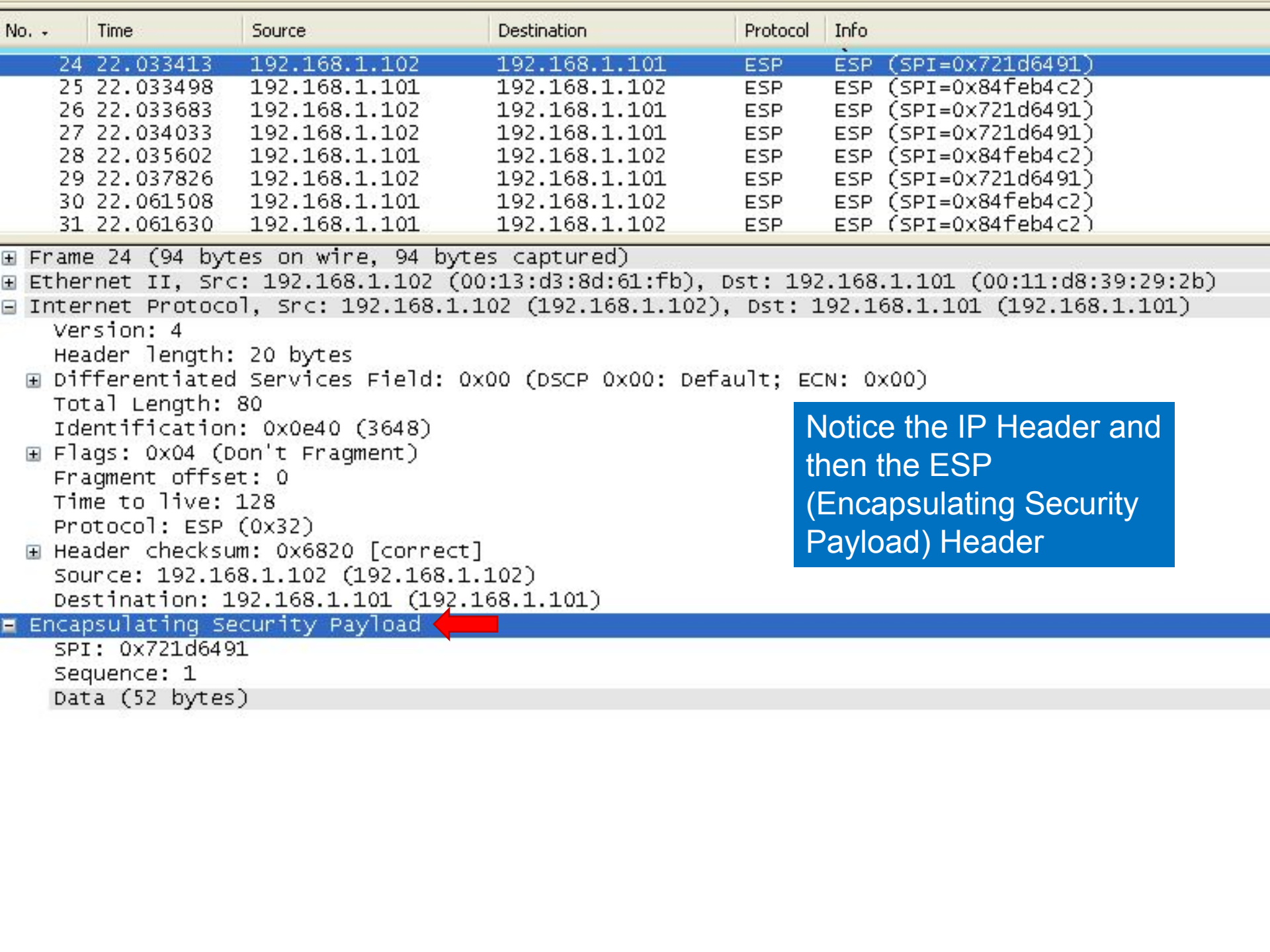
Use of Destination Options in Mobile IPv6

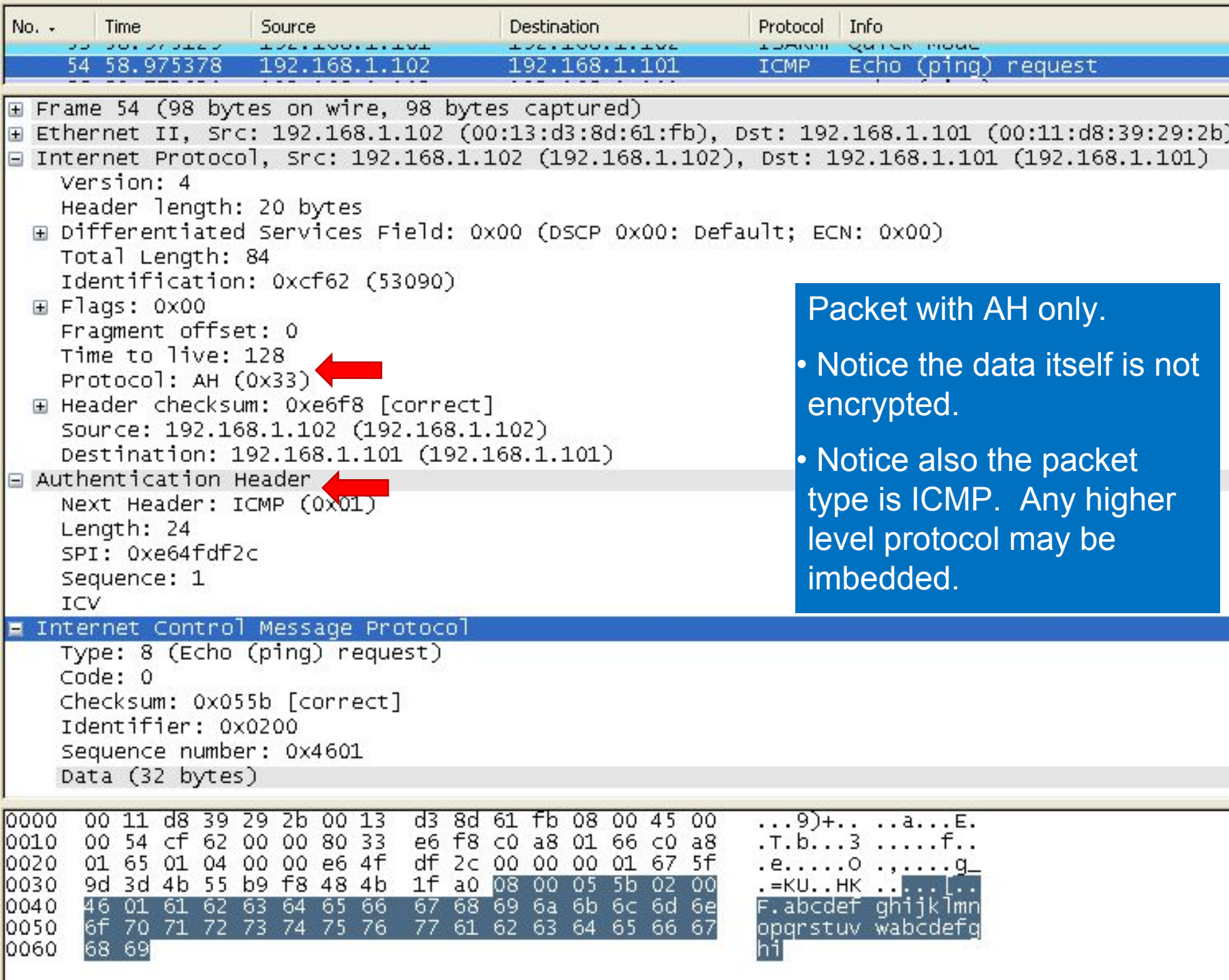

No. Time Source Destination
1 0.000000 3001::200:10ff:fe10:1181 3000::200:10ff:fe10:1060
Frame 1: 119 bytes on wire (952 bits), 119 bytes captured (952 bits)
Ethernet II, Src: Hughes_10:10:60 (00:00:10:10:10:60), Dst: IntelCor_16:c7:fe (00:15:17:16:c7
Internet Protocol Version 6, Src: 3001::200:10ff:fe10:1181 (3001::200:10ff:fe10:1181), Dst:
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00000000
.... 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
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)

- RH0 : can create routing loops.
- Deprecated
- Segments Left = zero, ignore
- Segments Left > zero, send ICMPv6 error message

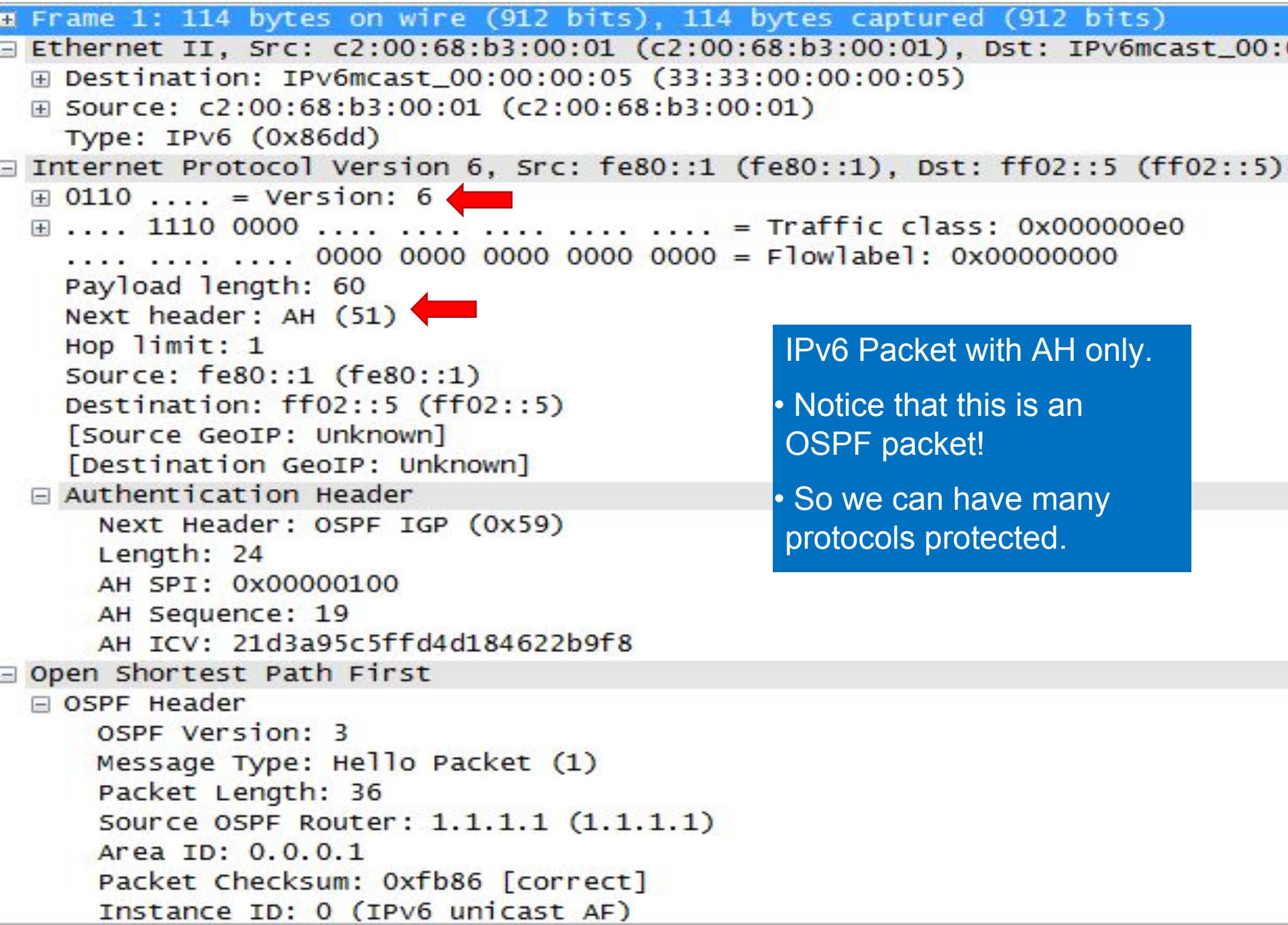



No. Time Source Destination Protocol Info
24 22.033413 192.168.1.102 192.168.1.101 ESP ESP (SPI=0x721d6491)
25 22.033498 192.168.1.101 192.168.1.102 ESP ESP (SPI=0x84feb4c2)
26 22.033683 192.168.1.102 192.168.1.101 ESP ESP (SPI=0x721d6491)
27 22.034033 192.168.1.102 192.168.1.101 ESP ESP (SPI=0x721d6491)
28 22.035602 192.168.1.101 192.168.1.102 ESP ESP (SPI=0x84feb4c2)
29 22.037826 192.168.1.102 192.168.1.101 ESP ESP (SPI=0x721d6491)
30 22.061508 192.168.1.101 192.168.1.102 ESP ESP (SPI=0x84feb4c2)
31 22.061630 192.168.1.101 192.168.1.102 ESP ESP (SPI=0x84feb4c2)
Frame 24 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: 192.168.1.102 (00:13:d3:8d:61:fb), Dst: 192.168.1.101 (00:11:d8:39:29:2b)
Internet Protocol, Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.101 (192.168.1.101)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 80
Identification: 0x0e40 (3648)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: ESP (0x32)
Header checksum: 0x6820 [correct]
Source: 192.168.1.102 (192.168.1.102)
Destination: 192.168.1.101 (192.168.1.101)
Encapsulating Security Payload
SPI: 0x721d6491
Sequence: 1
Data (52 bytes)
Notice the IP Header and then the ESP (Encapsulating Security Payload) Header



Packet with AH only.

- Notice the data itself is not encrypted.
- Notice also the packet type is ICMP. Any higher level protocol may be imbedded.

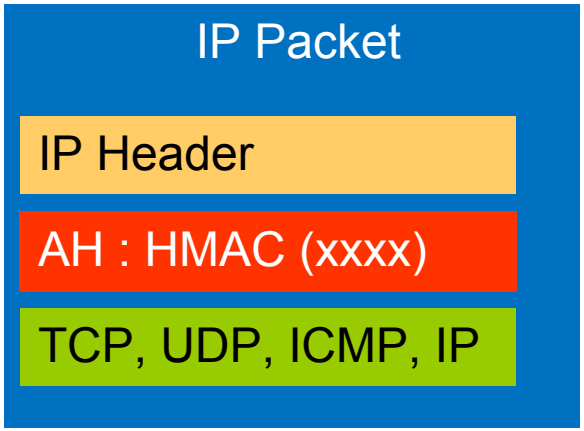


IPv6 Packet with AH only.

- Notice that this is an OSPF packet!
- So we can have many protocols protected.

Authentication Header

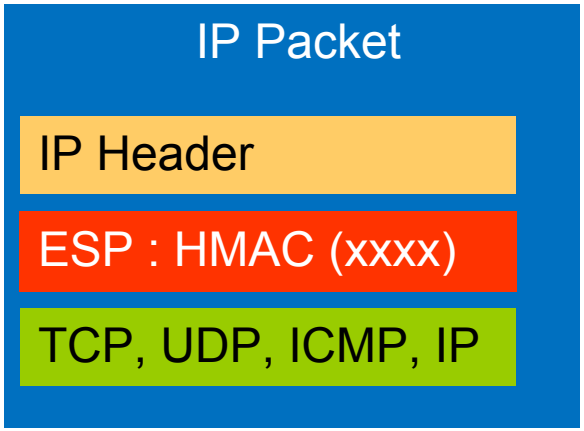
- Integrity: hash algorithms (ex. MD5 or SHA)
- The inputs to the hash algorithm are:
  - a secret key,
  - the payload of the packet, and
  - the unchangeable parts of the IP header, like the IP addresses.
- Source authentication: secret key
- Replay protection (optional): sequence numbers
- No encryption



- 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)
- Encryption □ hash □ generate ESP header



With ESP, the upper level protocol data is encrypted using the chosen algorithm.

Issues

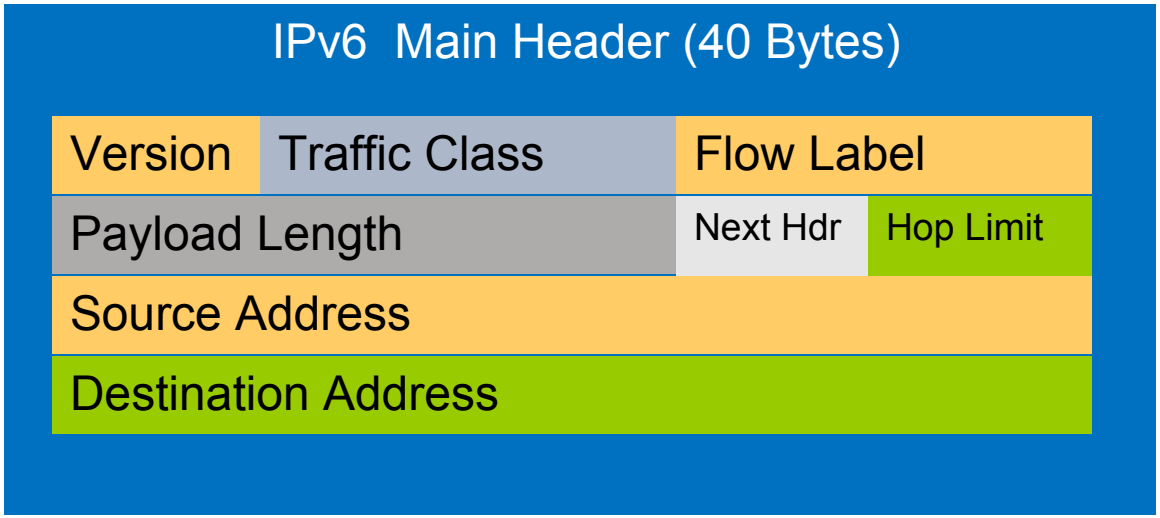
- Routers may drop
- Extension headers may be too big (ASIC size)
- Privacy violations
- Change the extension header not at source
- Parsing of TLV (Type, length, value)

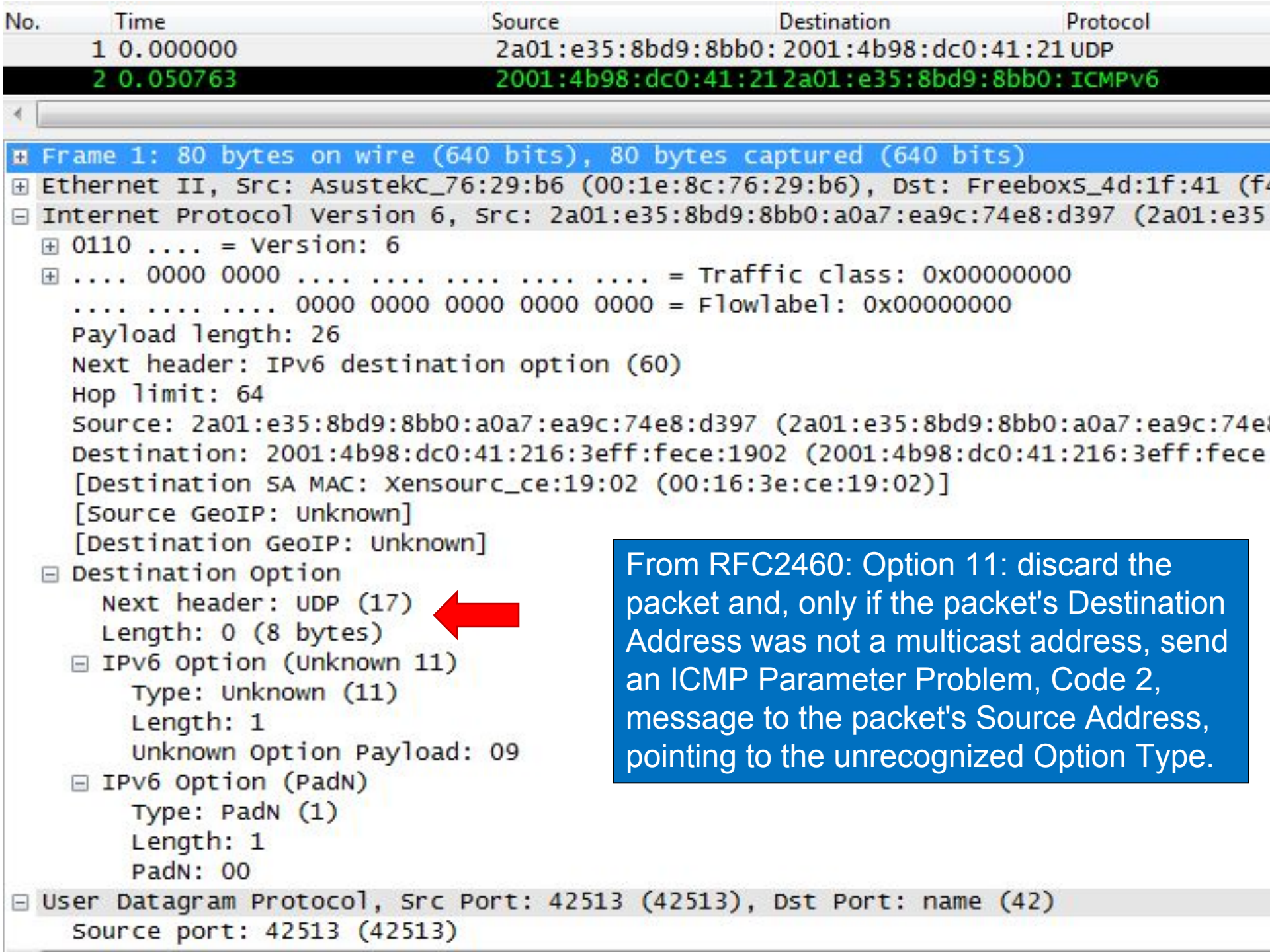
Pros

- 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

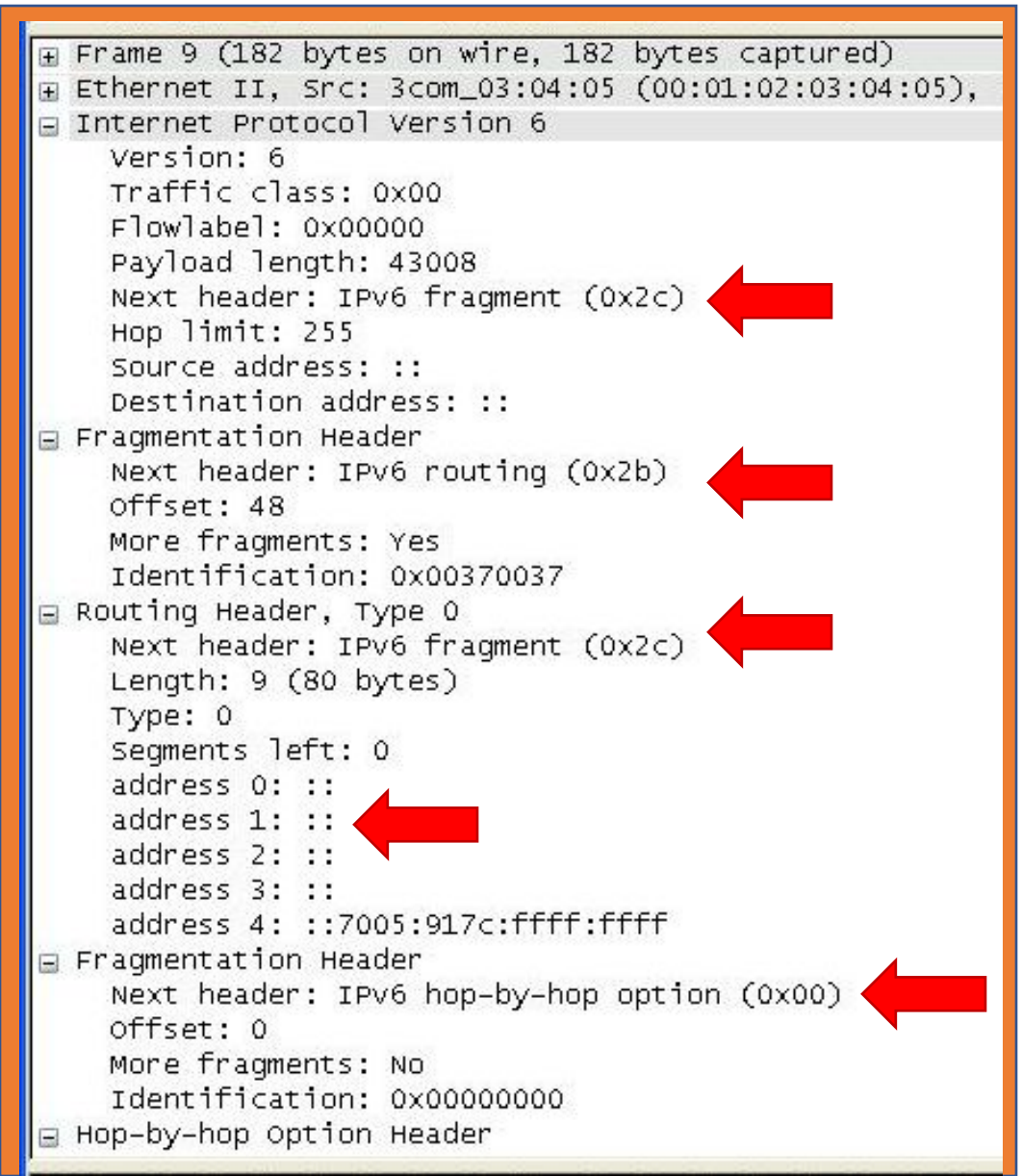
Malformed Packets

- Manipulate headers
  - IPv6 incorrect or partial header
  - Violate header order
  - Violate header option restrictions




No. Time Source Destination Protocol
1 0.000000 2a01:e35:8bd9:8bb0: 2001:4b98:dc0:41:21 UDP
2 0.050763 2001:4b98:dc0:41:21 2a01: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 (f
Internet Protocol Version 6, Src: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00000000
.... 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:74e
Destination: 2001:4b98:dc0:41:216:3eff:fece:1902 (2001:4b98:dc0:41:216:3eff:fece
[Destination SA MAC: Xensourc_ce:19:02 (00:16:3e:ce:19:02)]
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Destination Option
Next header: UDP (17)
Length: 0 (8 bytes)
IPv6 Option (Unknown 11)
Type: Unknown (11)
Length: 1
Unknown Option Payload: 09
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)
From RFC2460: Option 11: discard the packet and, only if the packet's Destination Address was not a multicast address, send an ICMP Parameter Problem, Code 2, message to the packet's Source Address, pointing to the unrecognized Option Type.

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…

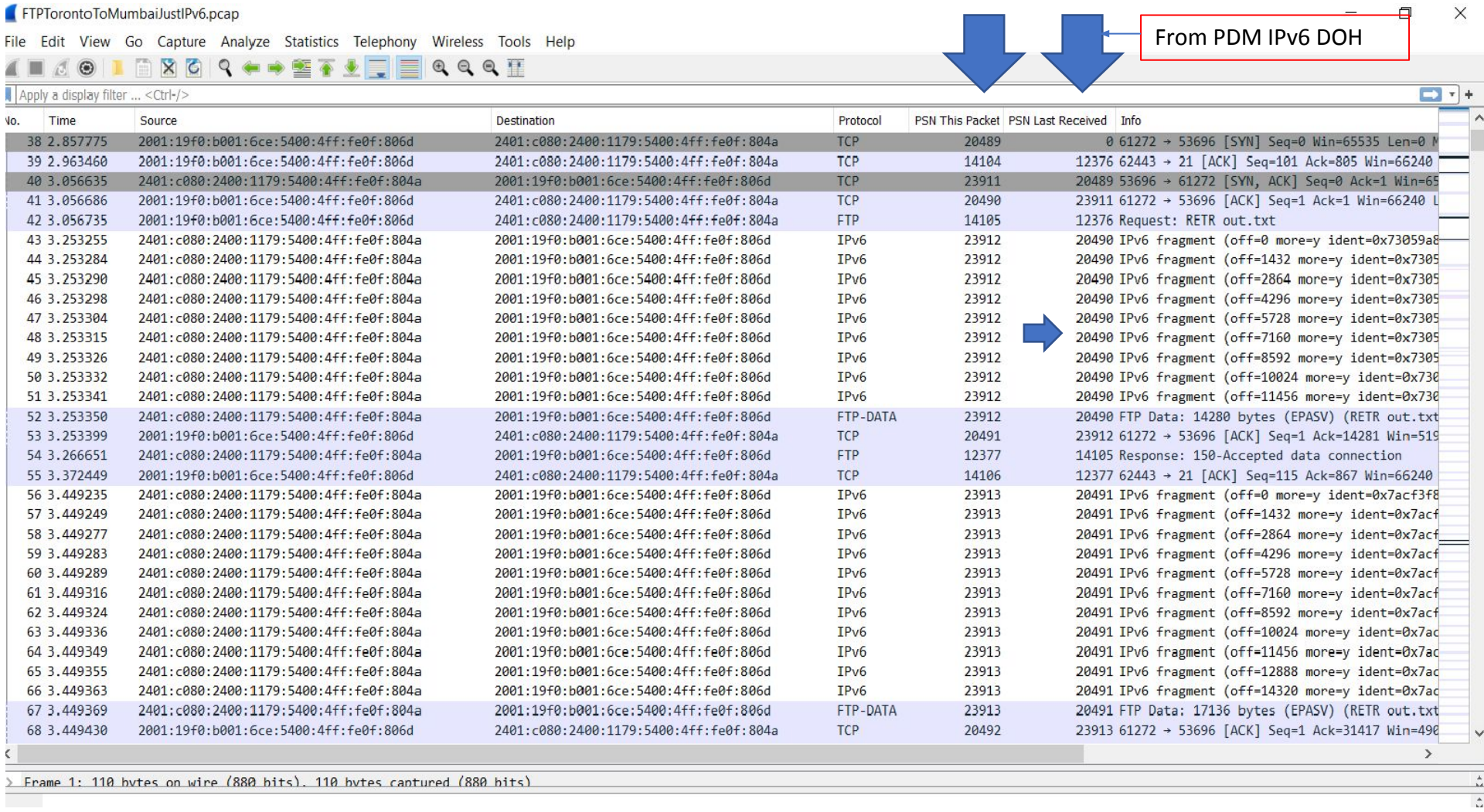
In particular, Dr. Mohit Tahiliani

Tested large FTP: Toronto to Mumbai (with PDM)

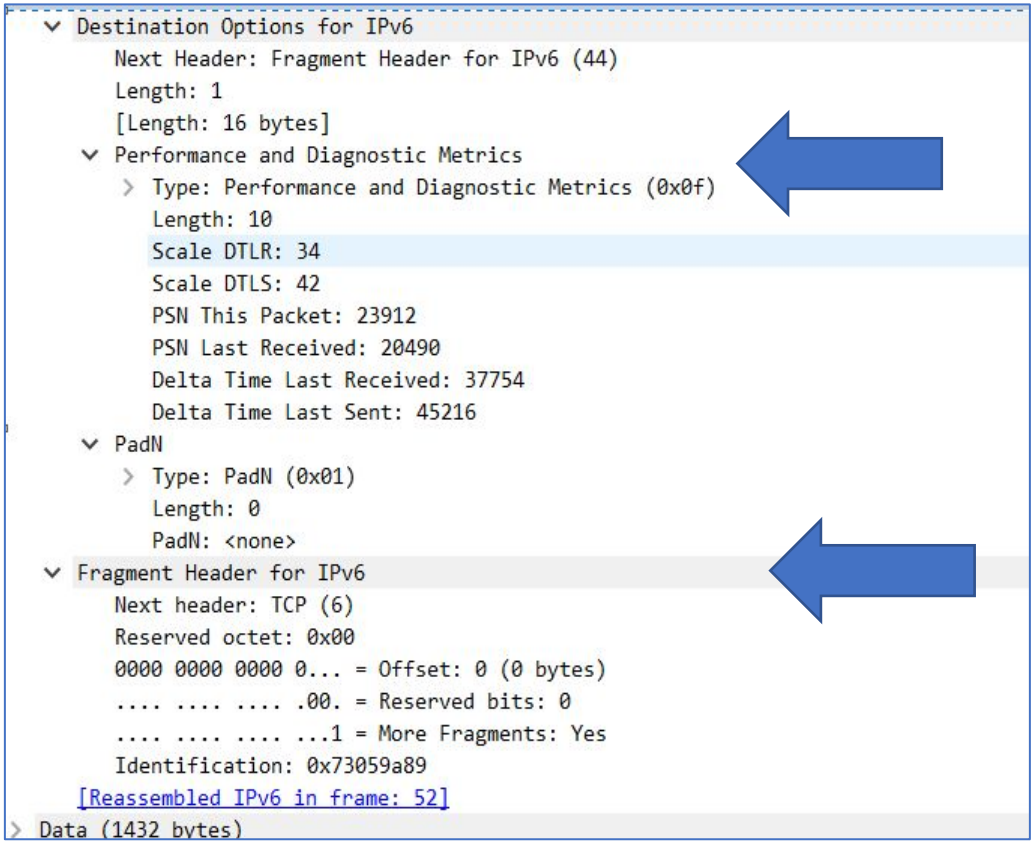
- Connected to **2401:c080:2400:1179:5400:04ff:fe0f:804a.**
- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
- 220-You are user number 1 of 50 allowed.
- 220-Local time is now 15:12. Server port: 21.
- 220 You will be disconnected after 15 minutes of inactivity.
- 331 User PDMuser OK. 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**
- 100% |**********| 27872 KiB 222.31 KiB/s 00:00 ETA
- 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



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

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!

Questions?

Contact:

info@iiesoc.in

president@industrynetcouncil.org

IPv4 – IPv6 Protocol Differences

IPv4	IPv6
1. Source and destination addresses are 32 bits (4 bytes) in length.	1. Source and destination addresses are 128 bits (16 bytes) in length
2. Fragmentation is supported at originating hosts and at intermediate routers.	2. Fragmentation is not supported at routers. It is only supported at the originating host.
3. IP header includes a checksum.	3. IP header does not include a checksum.
4. IP header includes options.	4. All optional data is moved to IPv6 extension headers.
5. IPsec support is not mandatory.	5. IPsec support is required in a full IPv6 implementation.
6. No identification of payload for QoS handling by routers is present within the IPv4 header.	6. Payload identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
7. In IPv4, the minimum MTU for routers and physical links is 576 bytes.	7. In IPv6, all links must handle a minimum MTU 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	Destination Address	The receiver of the packet