

IPv6 Trace Reading

NALINI ELKINS

INDUSTRY NETWORK TECHNOLOGY COUNCIL

PRESIDENT@INDUSTRYNETCOUNCIL.ORG



INTC Project

- Industry Network Technology Council (INTC)
- Funding: Grant from ARIN
- Thank you!



<https://www.iiesoc.in/>

<https://industriynetcouncil.org/>

Vision

Multi-year project: IPv6 deployment at enterprises.

Collaboration with American Registry for Internet Numbers (ARIN)

- Provide training,
- Analysis of security and application conversion,
- Help enterprises plan their IPv6 deployment.

Classes

- Introduction to IPv6 : Feb 4, 2021
- Lab: IPv6 basics : Feb 11, 2021
- Neighbor Discovery: March 4, 2021
- Lab: Neighbor Discovery: March 18, 2021
- IPv6 Address Planning: April 8, 2021
- Lab: IPv6 Address Planning: April 15, 2021
- IPv6 Transition Mechanisms: May 6, 2021
- Lab: IPv6 Transition Mechanisms: May 13, 2021

- DHCPv6: June 3, 2021
 - Lab: DHCPv6: June 10, 2021
 - IPv6 and Cloud: June 17, 2021
 - Lab: IPv6 and Cloud: June 24, 2021
 - Introduction to IPv6 Security July 8, 2021
- The next sessions are sponsored by a generous grant from ARIN.
- Trace Reading: August 12, 2021
 - Troubleshooting: August 19, 2021

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

Intro to Trace Reading

- Addresses
- Interfaces
- Payload

IPv4 address structure

IPv6 address structure

- Changes
- Flow label

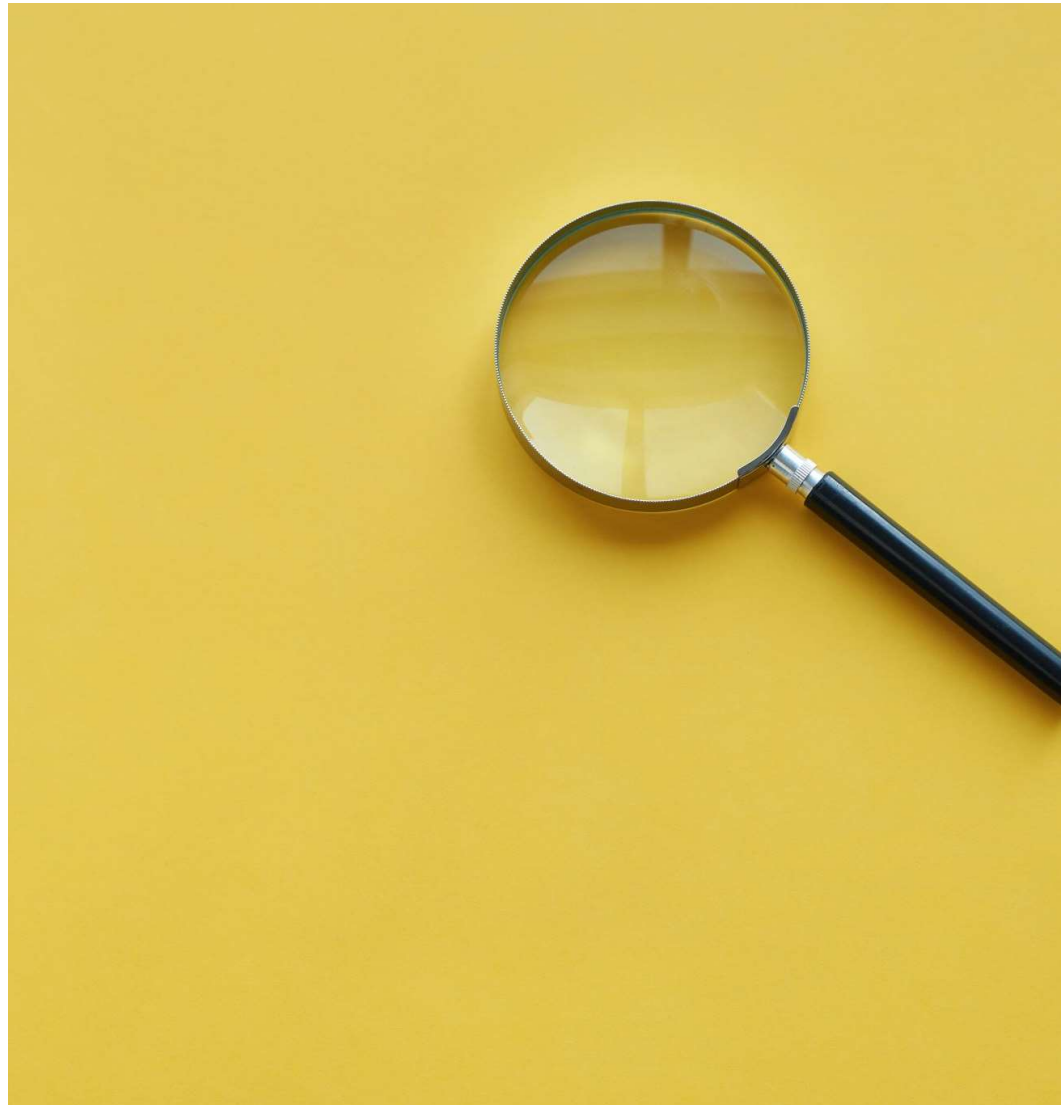
IPv6 extension headers

- Hop-by-hop
- Fragment
- Destination Options header
- 6LoWPAN

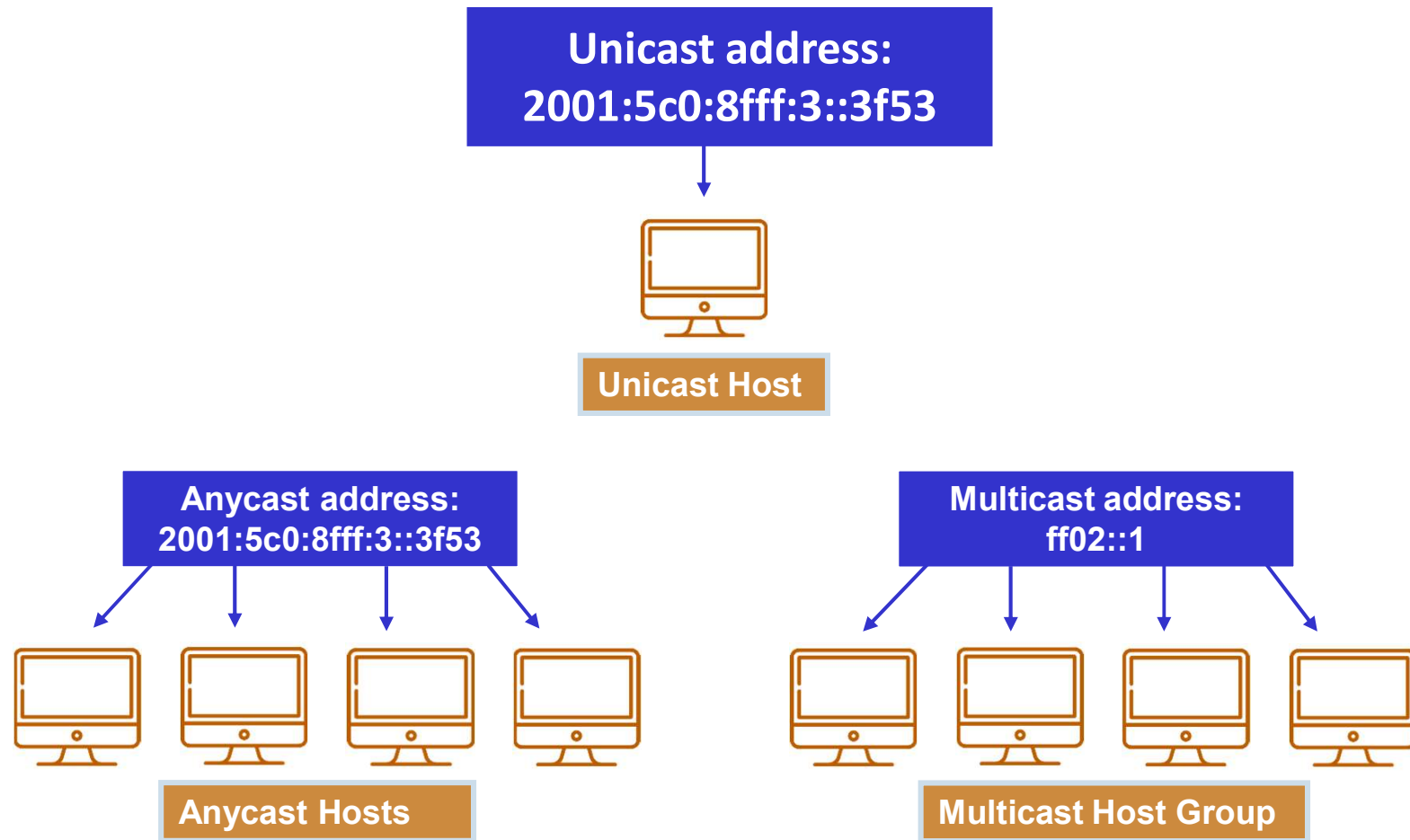
Security issues (header)

- Malformed packets
- Routing header

Know
the
protocol
... Know
how to
read a
trace!



IPv6 Address Types



Anycast addresses appear the same as unicast addresses

Importance of IPv6 Network Prefix

- First part of network prefix important!
- Example: **2001**:5c0:8fff:3::3f53
- Learn:
 - Can you go out on the internet with it,
 - What devices can you talk to,
 - Is it for special function.

FE80 = Link Local

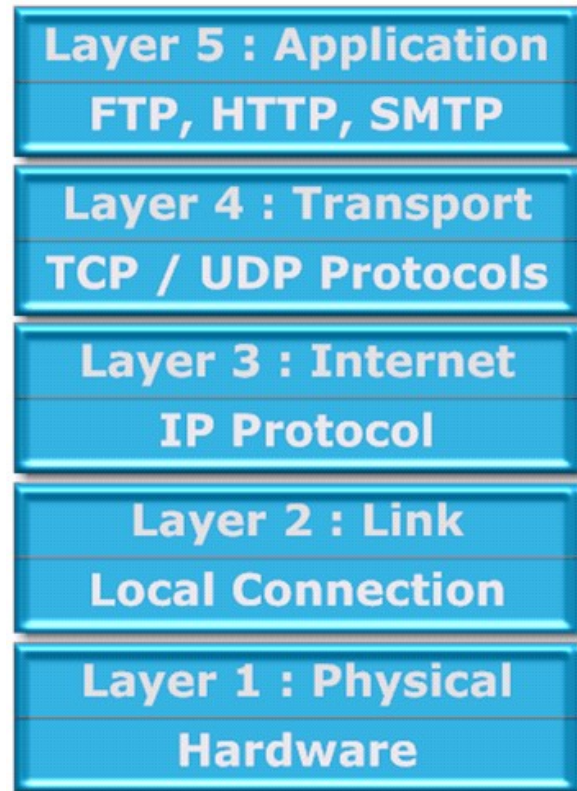
FFxx = Multicast

2001 = Global Unicast

0000 = Special

TCP/IP Layer Structure

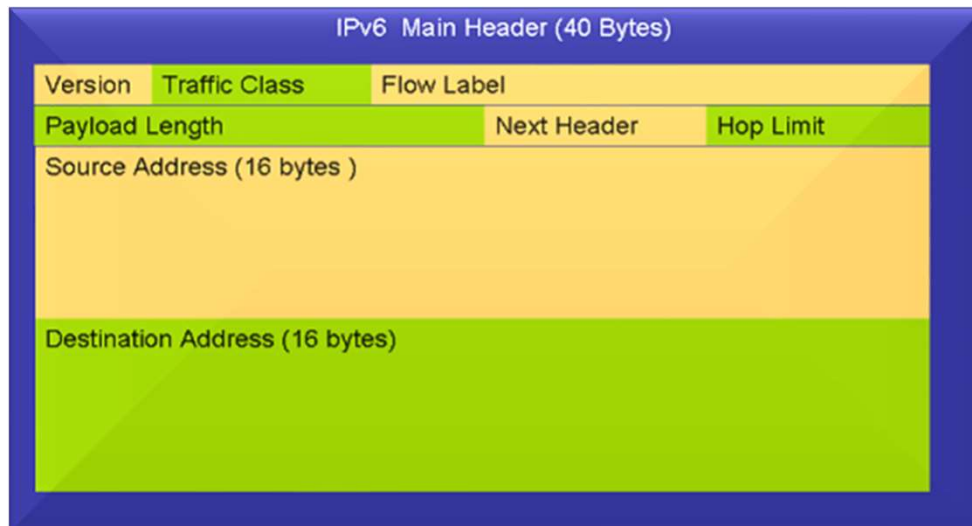
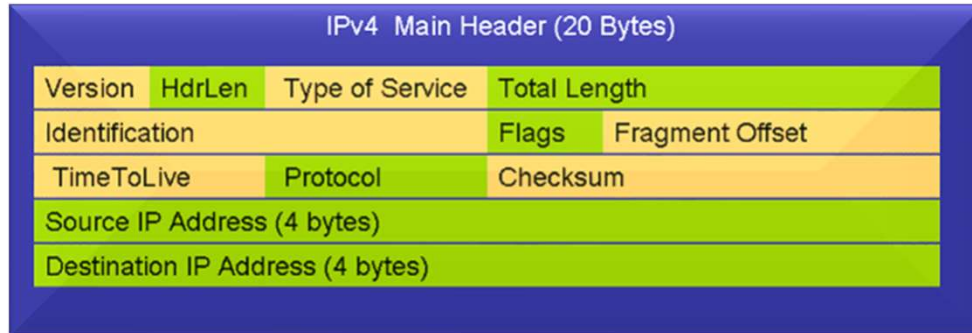
- TCP/IP layer structure
- Different levels for separation
- Each layer has a job



Packet Trace

No.	Time	Source	Destination
1	0.000000000	fe80::b4fe:58ff:fe80:2c78	ff02::1:2
Frame 1: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface br0, id 0			
Ethernet II, Src: HewlettP_77:31:04 (84:a9:3e:77:31:04), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)			
Destination: IPv6mcast_01:00:02 (33:33:00:01:00:02)			
Source: HewlettP_77:31:04 (84:a9:3e:77:31:04)			
Type: IPv6 (0x86dd)			
Internet Protocol Version 6, Src: fe80::b4fe:58ff:fe80:2c78, Dst: ff02::1:2			
0110 = Version: 6			
.... 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)			
.... 0001 0011 1100 0000 0001 = Flow Label: 0x13c01			
Payload Length: 83			
Next Header: UDP (17)			
Hop Limit: 1			
Source Address: fe80::b4fe:58ff:fe80:2c78			
Destination Address: ff02::1:2			
User Datagram Protocol, Src Port: 546, Dst Port: 547			
DHCPv6			
Message type: Solicit (1)			
Transaction ID: 0x61772d			
Rapid Commit			
Identity Association for Non-temporary Address			
Client Fully Qualified Domain Name			
Option Request			
Client Identifier			
Elapsed time			

IPv4 and IPv6 Headers



What is the same?

What is different?

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

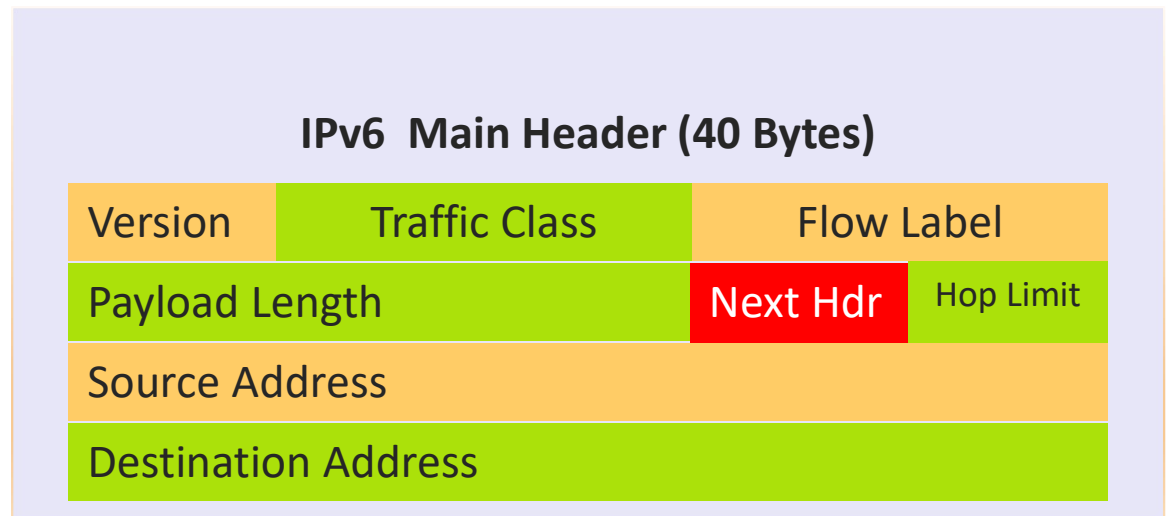
The IPv6 Header

IPv6 main header: fixed 40 bytes

Required

Source and destination addresses larger!

Defined in RFC2460



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

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!

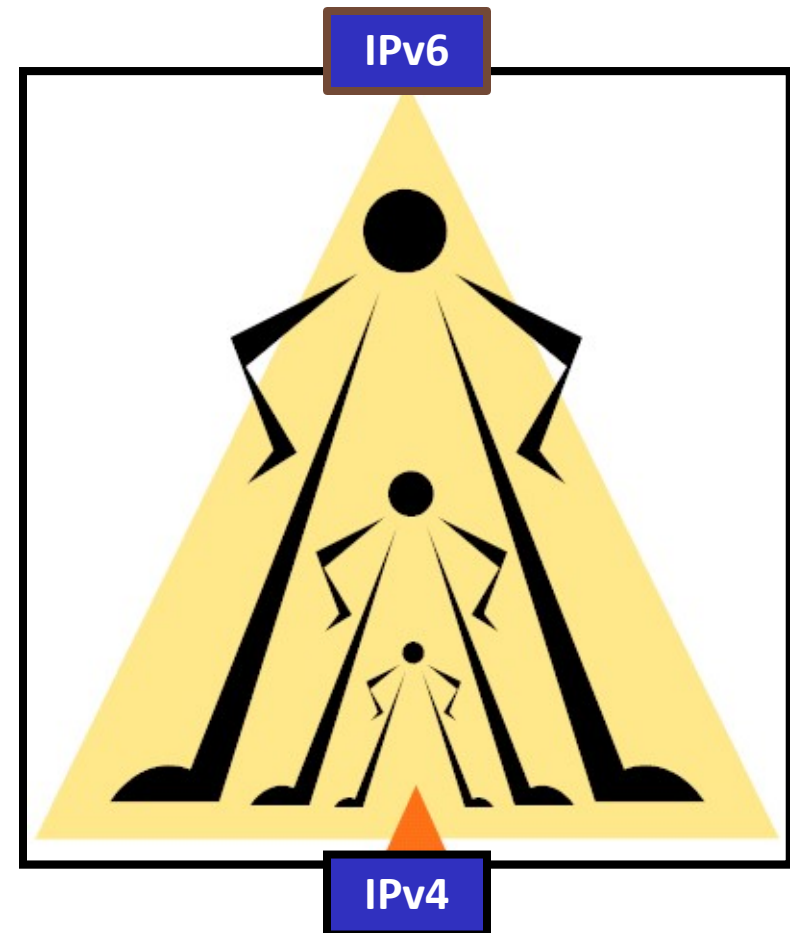
What Did They Do?

Multiple header structure

Took out fields

Added some fields

Renamed fields



IPv6 Header Changes Summary

The changes for the IPv6 main header are:

Unchanged Fields: Three fields used same way and have same name (size may be different!): *Version*, *Source Address* and *Destination Address*.

Renamed Fields: Two fields used same way but renamed: *Traffic Class* and *Hop Limit*.

Changed Fields: Two fields used similar way and renamed: *Payload Length* and *Next Header*.

Added Fields: One new field: *Flow Label*.

Removed Fields: Five fields removed:

- **Header Length:** Not needed (IPv6 main header is fixed at 40 bytes)
- **Identification, Flags, Fragment Offset:** Moved to Fragment extension header
- **Header Checksum:** Eliminated

IPv4 Options : moved to extension headers (if used)

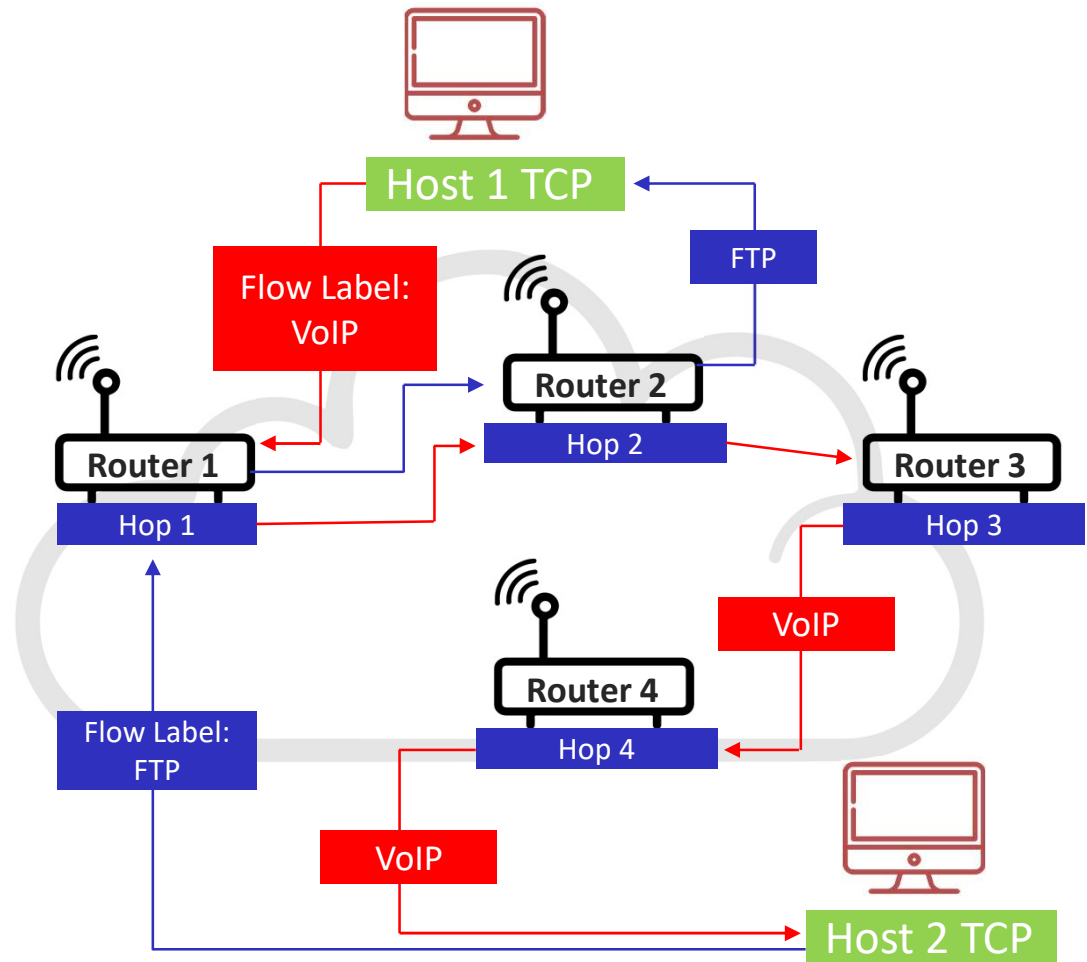
Flow Label

Quality of Service

What is a flow?

All routers on the path

SNA CoS



Trace Packet With Flow Label

No.	Time	Source	Destination	Protocol	Len
3406	64.672910	2607:f4e8:130:202:225:90ff:fe01:a610	2607:f740:0:3f:216:3eff:fe68:72c0	TCP	

Frame 3406: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)

Ethernet II, Src: Cisco_ae:30:0a (00:0c:cf:ae:30:0a), Dst: Xensourc_68:72:c0 (00:16:3e:68:72:c0)

Internet Protocol Version 6, Src: 2607:f4e8:130:202:225:90ff:fe01:a610 (2607:f4e8:130:202:225:90ff:fe01:a610),
0110 = Version: 6
.... 0000 0000 = Traffic class: 0x00000000
.... 1001 0011 1001 0010 1110 = Flowlabel: 0x0009392e
Payload length: 40
Next header: TCP (0x06)
Hop limit: 56
Source: 2607:f4e8:130:202:225:90ff:fe01:a610 (2607:f4e8:130:202:225:90ff:fe01:a610)
[Source SA MAC: SuperMic_01:a6:10 (00:25:90:01:a6:10)]
Destination: 2607:f740:0:3f:216:3eff:fe68:72c0 (2607:f740:0:3f:216:3eff:fe68:72c0)
[Destination SA MAC: Xensourc_68:72:c0 (00:16:3e:68:72:c0)]

Transmission Control Protocol, Src Port: http (80), Dst Port: 41991 (41991), Seq: 0, Ack: 1, Len: 0
Source port: http (80)
Destination port: 41991 (41991)
[Stream index: 43]
Sequence number: 0 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 40 bytes
Flags: 0x012 (SYN, ACK)
window size value: 65535
[Calculated window size: 65535]
Checksum: 0xff36 [validation disabled]
Options: (20 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

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)

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)

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

No.	Time	Source	Destination
5762	80.385670	2001:4998:0:6::15	2607:f740:0:3f:216:3eff:fe68:72c0

Frame 5762: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits)

Ethernet II, Src: Cisco_ae:30:0a (00:0c:cf:ae:30:0a), Dst: Xensourc_68:72:c0

Internet Protocol Version 6, Src: 2001:4998:0:6::15 (2001:4998:0:6::15), Dst: 2607:f740:0:3f:216:3eff:fe68:72c0 (2607:f740:0:3f:216:3eff:fe68:72c0)

- 0110 = Version: 6
- 0000 0000 = Traffic class: 0x00000000
- 0101 0100 0001 0000 1100 = Flowlabel: 0x0005410c

Payload length: 1440 ←

Next header: IPv6 fragment (0x2c) ←

Hop limit: 56

Source: 2001:4998:0:6::15 (2001:4998:0:6::15)

Destination: 2607:f740:0:3f:216:3eff:fe68:72c0 (2607:f740:0:3f:216:3eff:fe68:72c0)

[Destination SA MAC: Xensourc_68:72:c0 (00:16:3e:68:72:c0)]

Fragmentation Header ←

- Next header: TCP (0x06)
- 0000 0000 0000 0... = offset: 0 (0x0000)
- 1 = More Fragment: Yes
- Identification: 0xa262a3bc

[Reassembled 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

```
⊞ 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 (old) (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	Protocol	Length	Info
1	0.000000	2a01:e35:8bd9:8bb0:	2001:4b98:dc0:41:21	UDP	80	Source port:
2	0.050763	2001:4b98:dc0:41:21	2a01:e35:8bd9:8bb0:	ICMPv6	128	Destination

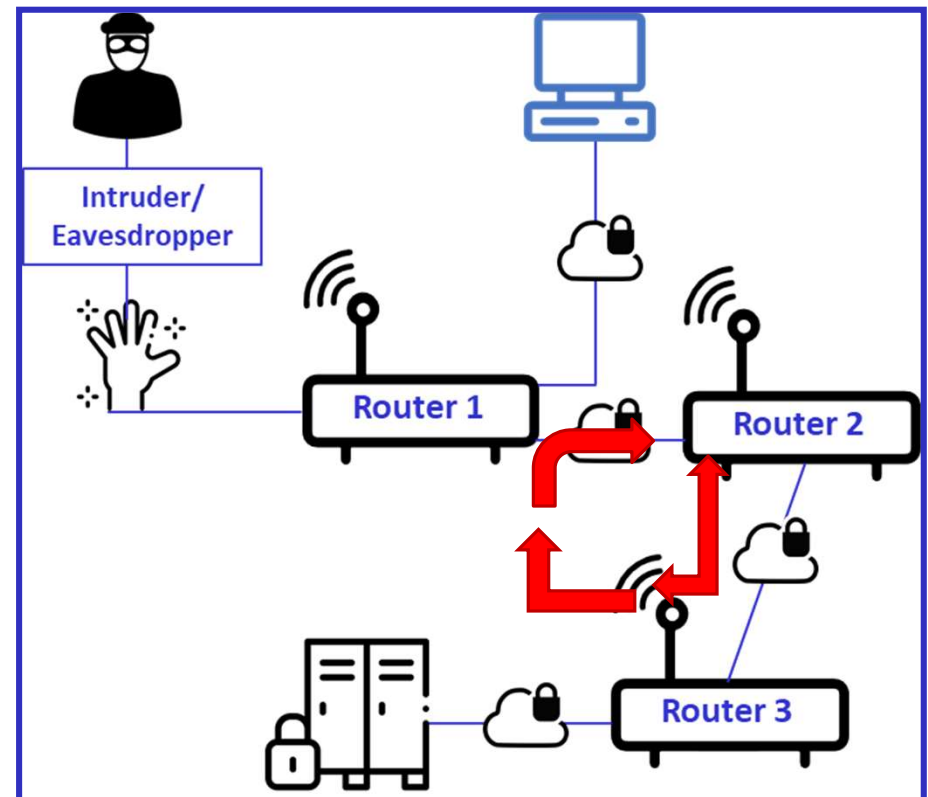
Frame 1: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)

- ⊕ Ethernet II, Src: AsustekC_76:29:b6 (00:1e:8c:76:29:b6), Dst: FreeboxS_4d:1f:41 (f4:ca:e5:4d:1f:41)
- ⊖ Internet Protocol version 6, Src: 2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397 (2a01:e35:8bd9:8bb0:a0a7:ea9c:74e8:d397),
 - ⊕ 0110 = Version: 6
 - ⊕ 0000 0000 = Traffic class: 0x00000000
 - 0000 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:d397)
 - Destination: 2001:4b98:dc0:41:216:3eff:fece:1902 (2001:4b98:dc0:41:216:3eff:fece:1902)
 - [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.

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

No. -	Time	Source	Destination	Protocol	Info
54	58.975378	192.168.1.102	192.168.1.101	ICMP	Echo (ping) request

```

+ Frame 54 (98 bytes on wire, 98 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: 84
  Identification: 0xcf62 (53090)
  + Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: AH (0x33)
  + Header checksum: 0xe6f8 [correct]
  Source: 192.168.1.102 (192.168.1.102)
  Destination: 192.168.1.101 (192.168.1.101)
- Authentication Header
  Next Header: ICMP (0x01)
  Length: 24
  SPI: 0xe64fdf2c
  Sequence: 1
  ICV
- Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x055b [correct]
  Identifier: 0x0200
  Sequence number: 0x4601
  Data (32 bytes)

```

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.

```

0000  00 11 d8 39 29 2b 00 13 d3 8d 61 fb 08 00 45 00  ...9)+.. ..a...E.
0010  00 54 cf 62 00 00 80 33 e6 f8 c0 a8 01 66 c0 a8  .T.b...3 .....f..
0020  01 65 01 04 00 00 e6 4f df 2c 00 00 00 01 67 5f  .e.....0 .....,g_
0030  9d 3d 4b 55 b9 f8 48 4b 1f a0 08 00 05 5b 02 00  .=KU..HK .....[..
0040  46 01 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e  F.abcdef ghijklmn
0050  6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67  opqrstuv wabcdefg
0060  68 69  hi

```

```

# 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 (33:33:00:00:00:05)
  # 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 ←
  # .... 1110 0000 .... .... .... = Traffic class: 0x000000e0
  # .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 60
  Next header: AH (51) ←
  Hop limit: 1
  Source: fe80::1 (fe80::1)
  Destination: ff02::5 (ff02::5)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
# Authentication Header
  Next Header: OSPF IGP (0x59)
  Length: 24
  AH SPI: 0x00000100
  AH Sequence: 19
  AH ICV: 21d3a95c5ffd4d184622b9f8
# Open Shortest Path First
  # OSPF Header
    OSPF 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)

```

IPv6 Packet with AH only.

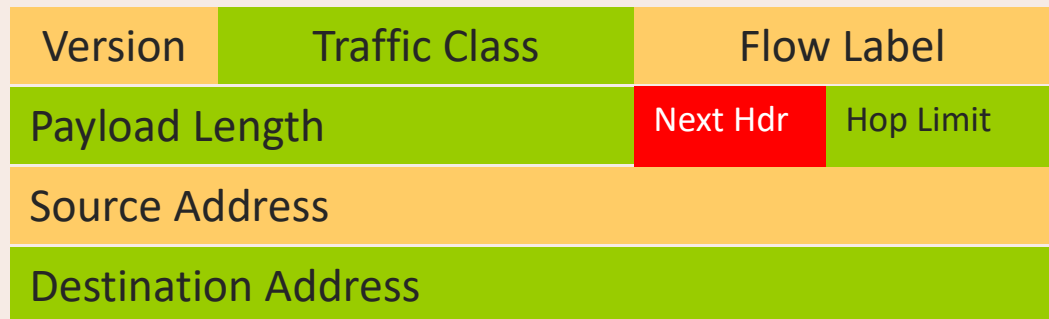
- Notice that this is an OSPF packet!
- So we can have many protocols protected.

Malformed Packets

Manipulate headers

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

IPv6 Main Header (40 Bytes)



Crafted Packet

```
⊕ Frame 9 (182 bytes on wire, 182 bytes captured)
⊕ Ethernet II, Src: 3com_03:04:05 (00:01:02:03:04:05),
⊖ Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 43008
  Next header: IPv6 fragment (0x2c) ←
  Hop limit: 255
  Source address: ::
  Destination address: ::
⊖ Fragmentation Header
  Next header: IPv6 routing (0x2b) ←
  Offset: 48
  More fragments: Yes
  Identification: 0x00370037
⊖ Routing Header, Type 0
  Next header: IPv6 fragment (0x2c) ←
  Length: 9 (80 bytes)
  Type: 0
  Segments left: 0
  address 0: ::
  address 1: :: ←
  address 2: ::
  address 3: ::
  address 4: ::7005:917c:ffff:ffff
⊖ Fragmentation Header
  Next header: IPv6 hop-by-hop option (0x00) ←
  Offset: 0
  More fragments: No
  Identification: 0x00000000
⊖ Hop-by-hop option Header
```

Crafted IPv6 packet

Multiple headers

Deprecated headers

Headers out of order

6LoWPAN Header

6LoWPAN stands for *IPv6 over Low Power Wireless Personal Area Networks (RFC4919)*

Meant for very low power devices.

Small packet size: 127 bytes

Header compression

From RFC4944

IPv6 over IEEE 802.15.4

Whereas in an IPv6 header the stack would contain, in the following order, addressing, hop-by-hop options, routing, fragmentation, destination options, and finally payload [[RFC2460](#)]; in a LoWPAN header, the analogous header sequence is mesh (L2) addressing, hop-by-hop options (including L2 broadcast/multicast), fragmentation, and finally payload.

Sample 6LoWPAN Header

```
Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits)
Ethernet II, Src: ExeginTe_00:10:04 (00:1c:da:00:10:04), Dst: Dell_10:30:e5 (00:22:...)
Internet Protocol Version 4, Src: 172.16.1.144 (172.16.1.144), Dst: 172.16.1.52 (172.16.1.52)
User Datagram Protocol, Src Port: zep (17754), Dst Port: zep (17754)
ZigBee Encapsulation Protocol, Channel: 3, Length: 43 ←
IEEE 802.15.4 Data, Dst: Broadcast, Src: 0x5566 ←
6LOWPAN
  IPHC Header
    011. .... = Pattern: IP header compression (0x03)
    ...1 1... .... = Traffic class and flow label: version, traffic class, and
    .... .0.. .... = Next header: inline
    .... ..11 .... = Hop limit: 255 (0x0003)
    .... .... 0... .... = Context identifier extension: False
    .... .... .0.. .... = Source address compression: Stateless
    .... .... ..11 .... = Source address mode: Compressed (0x0003)
    .... .... .... 1... = Multicast address compression: True
    .... .... .... .0.. = Destination address compression: Stateless
    .... .... .... ..11 = Destination address mode: 8-bits inline (0x0003)
    Next header: ICMPv6 (0x3a)
    Source: fe80::ff:fe00:5566 (fe80::ff:fe00:5566)
    Destination: ff02::1a (ff02::1a)
  Internet Protocol Version 6, Src: fe80::ff:fe00:5566 (fe80::ff:fe00:5566), Dst: ff02::1a (ff02::1a)
  Internet Control Message Protocol v6
    Type: RPL Control (155)
    Code: 1 (DODAG Information Object)
    Checksum: 0x7545 [correct]
    RPLInstanceID: 0
    Version: 241
    Rank: 858
  Flags: 0x8b
    Destination Advertisement Trigger Sequence Number (DTSN): 240
    Flags: 0x00
    Reserved: 00
    DODAGID: fd00::ff:fe00:1122 (fd00::ff:fe00:1122)
```

IPv6 Multicast Scope

- IPv6 multicast addresses start with FF.
- Last 4 bits is scope. (Ex. FF01, FF02, etc).
- FF01:: means on same interface
- FF02:: means on same link
- FF05:: means in the same site
- FF0E:: means in the Internet.

(From RFC 4291)

Common IPv6 Multicast Groups

- Multicast addresses are registered with the Internet Assigned Numbers Authority (IANA).

See:

<http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml>

<u>IPv6 multicast address</u>	<u>Description</u>
FF02::1	The all-nodes address
FF02::2	The all-routers address
FF02::5	The all-Open Shortest Path First (OSPF) routers address
FF02::6	The all-OSPF designated routers address



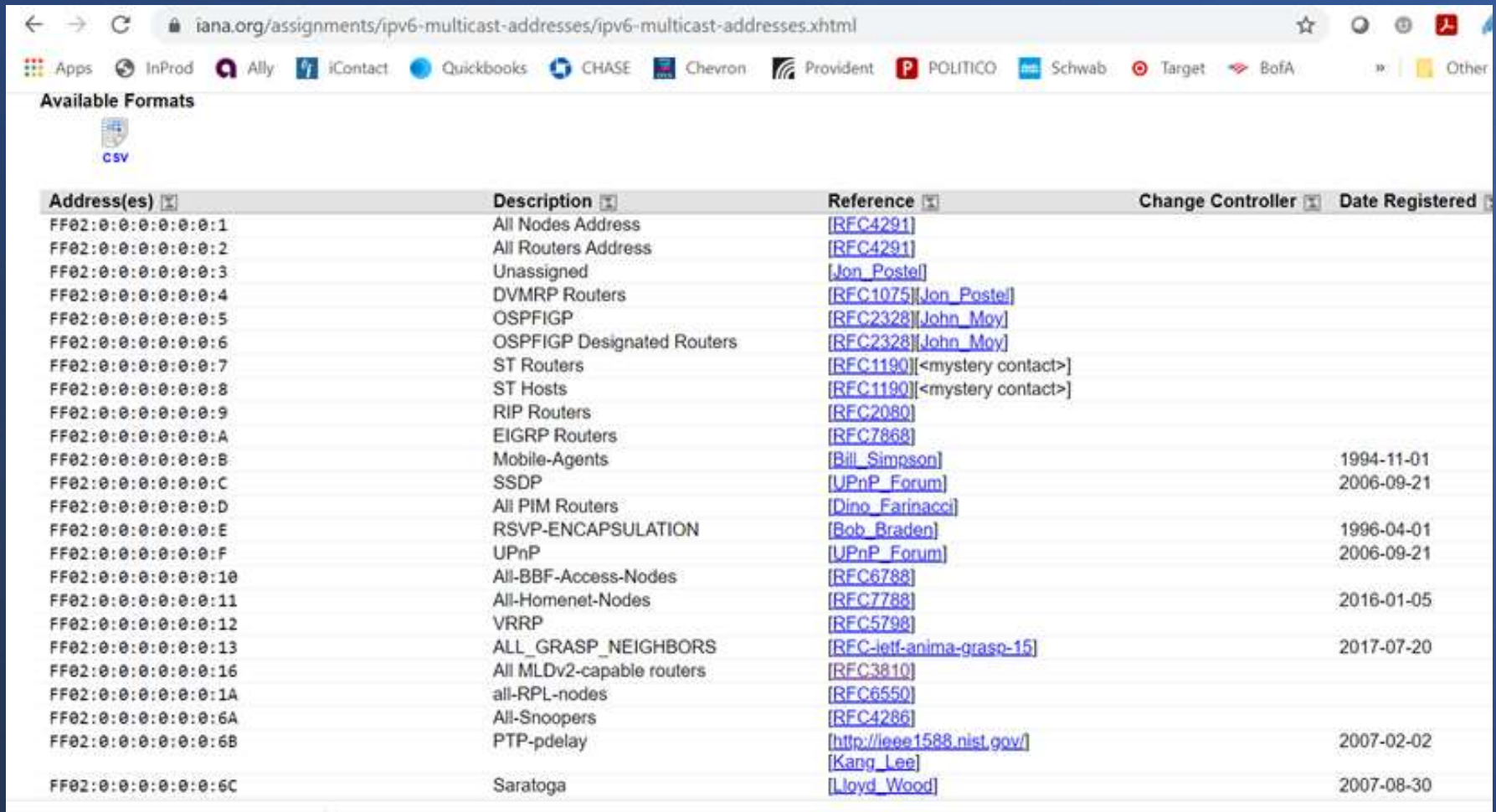
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination
115	99.0044030...	fe80::3a68:ddff:fe1a:c57d	ff02::c
116	99.0044702...	fe80::a94:efff:fe9a:c709	ff02::c
117	99.0044906...	2021:2021:2021:367:3a68:ddff:fe1a:642d	ff08::c
118	99.0048375...	fe80::3a68:ddff:fe1a:6525	ff02::c
119	99.0052046...	fe80::3a68:ddff:fe1a:642d	ff02::c
120	99.1283638...	2021:2021:2021:367:3a68:ddff:fe1a:c105	ff08::c
121	99.1283996...	2021:2021:2021:367:3a68:ddff:fe1a:dba5	ff08::c
122	99.1286156...	fe80::3a68:ddff:fe1a:c105	ff02::c
123	99.1287661...	fe80::3a68:ddff:fe1a:dba5	ff02::c
124	99.2539717...	2021:2021:2021:367:3a68:ddff:fe1a:6525	ff08::c
125	99.2540748...	2021:2021:2021:367:a94:efff:fe9a:c709	ff08::c
126	99.2543223...	2021:2021:2021:367:3a68:ddff:fe1a:c57d	ff08::c
127	99.2548423...	fe80::3a68:ddff:fe1a:c57d	ff02::c
128	99.2549108...	fe80::a94:efff:fe9a:c709	ff02::c

<

- > Frame 115: 456 bytes on wire (3648 bits), 456 bytes captured (3648 bits) on interface br0, id 0
- > Ethernet II, Src: Inventec_1a:c5:7d (38:68:dd:1a:c5:7d), Dst: IPv6mcast_0c (33:33:00:00:00:0c)
- > Internet Protocol Version 6, Src: fe80::3a68:ddff:fe1a:c57d, Dst: ff02::c
- > User Datagram Protocol, Src Port: 1900, Dst Port: 1900
- ▼ **Simple Service Discovery Protocol**
 - > NOTIFY * HTTP/1.1\r\n
 - HOST: [FF02::C]:1900\r\n
 - SERVER: :2.70 UPnP/1.1 7X06CT01WW:J301D82R\r\n
 - NT: urn:dmtf-org:service:cedfish-rest:1.6\r\n

IANA IPv6 Multicast Groups



The screenshot shows a web browser window with the URL iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml. The page displays a table of IPv6 multicast addresses and their associated information. The table has five columns: Address(es), Description, Reference, Change Controller, and Date Registered. The data is as follows:

Address(es)	Description	Reference	Change Controller	Date Registered
FF02:0:0:0:0:0:0:1	All Nodes Address	[RFC4291]		
FF02:0:0:0:0:0:0:2	All Routers Address	[RFC4291]		
FF02:0:0:0:0:0:0:3	Unassigned	[Jon Postel]		
FF02:0:0:0:0:0:0:4	DVMRP Routers	[RFC1075] [Jon Postel]		
FF02:0:0:0:0:0:0:5	OSPFv2	[RFC2328] [John Moy]		
FF02:0:0:0:0:0:0:6	OSPFv2 Designated Routers	[RFC2328] [John Moy]		
FF02:0:0:0:0:0:0:7	ST Routers	[RFC1190] [<mystery contact>]		
FF02:0:0:0:0:0:0:8	ST Hosts	[RFC1190] [<mystery contact>]		
FF02:0:0:0:0:0:0:9	RIP Routers	[RFC2080]		
FF02:0:0:0:0:0:0:A	EIGRP Routers	[RFC7868]		
FF02:0:0:0:0:0:0:B	Mobile-Agents	[Bill Simpson]		1994-11-01
FF02:0:0:0:0:0:0:C	SSDP	[UPnP Forum]		2006-09-21
FF02:0:0:0:0:0:0:D	All PIM Routers	[Dino Farinacci]		
FF02:0:0:0:0:0:0:E	RSVP-ENCAPSULATION	[Bob Braden]		1996-04-01
FF02:0:0:0:0:0:0:F	UPnP	[UPnP Forum]		2006-09-21
FF02:0:0:0:0:0:0:10	All-BBF-Access-Nodes	[RFC6788]		
FF02:0:0:0:0:0:0:11	All-Homenet-Nodes	[RFC7788]		2016-01-05
FF02:0:0:0:0:0:0:12	VRRP	[RFC5798]		
FF02:0:0:0:0:0:0:13	ALL_GRASP_NEIGHBORS	[RFC-ietf-anima-grasp-15]		2017-07-20
FF02:0:0:0:0:0:0:16	All MLDv2-capable routers	[RFC3810]		
FF02:0:0:0:0:0:0:1A	all-RPL-nodes	[RFC6550]		
FF02:0:0:0:0:0:0:6A	All-Snoopers	[RFC4286]		
FF02:0:0:0:0:0:0:6B	PTP-pdelay	http://ieee1588.nist.gov/ [Kang Lee]		2007-02-02
FF02:0:0:0:0:0:0:6C	Saratoga	[Lloyd Wood]		2007-08-30

Questions?

Contact:

nalini.elkins@insidestack.com

president@industry.netcouncil.org

More webinars at:

industry.netcouncil.org