


IFT 266 Introduction to Network Information Communication Technology (ICT)

Lab 20

IPV6 Header

Objective: Analyze the IPv6 header in Wireshark

1. Open up Wireshark (you should have it already downloaded from your earlier networking course).

Completed 

2. We are going to use the www.cnn.com as our sample website.

Using the nslookup function that your previously learned my networking courses, what is the IPv6 address of cnn.com?

2600:8800:8000:207:c240:d0ff:fe87:2efa

3. Now using the ipconfig command, find your IPv6 GUA address

2600:8800:8000:207::1003

4. Now go back into Wireshark and do a capture when you search for www.cnn.com.

Completed 

5. Now look for your IPv6 address as the source and cnn.com's IPv6 address as the destination as in the image below,

No.	Time	Source	Destination	Protocol	Length	Info
29	1.392777	2a02:26f0:71:48b::...	2001:bb6:6972:e758...	TCP	74	443 → 53355 [ACK] Seq=1 Ac
30	1.392778	2a02:26f0:71:48b::...	2001:bb6:6972:e758...	TCP	74	443 → 53356 [ACK] Seq=1 Ac
32	1.395349	2001:bb6:6972:e758...	2a04:4e42:43::323	TCP	86	58260 → 443 [SYN] Seq=0 W
37	1.397440	2001:bb6:6972:e758...	2a04:4e42:400::323	TCP	86	58261 → 443 [SYN] Seq=0 W
43	1.406668	2a04:4e42:43::323	2001:bb6:6972:e758...	TCP	86	443 → 58260 [SYN, ACK] Sec
44	1.406814	2001:bb6:6972:e758...	2a04:4e42:43::323	TCP	74	58260 → 443 [ACK] Seq=1 Ac

Completed 

6. For this lab we will look at Packet 32 where both the source address and destination address are Global Unicast Addresses. We also that in the protocol field we have TCP packet.

We will now look down at the network layer information area and you will see that the IPv6 information has been expanded.

32	1.395349	2001:bb6:6972:e758...	2a04:4e42:43::323	TCP	86	58260 → 443	[SYN] Seq=0 W
37	1.397440	2001:bb6:6972:e758...	2a04:4e42:400::323	TCP	86	58261 → 443	[SYN] Seq=0 W
43	1.406668	2a04:4e42:43::323	2001:bb6:6972:e758...	TCP	86	443 → 58260	[SYN, ACK] Se
44	1.406814	2001:bb6:6972:e758...	2a04:4e42:43::323	TCP	74	58260 → 443	[ACK] Seq=1 A
49	1.407980	2a04:4e42:400::323	2001:bb6:6972:e758...	TCP	86	443 → 58261	[SYN, ACK] Se
50	1.408101	2001:bb6:6972:e758...	2a04:4e42:400::323	TCP	74	58261 → 443	[ACK] Seq=1 A
57	1.418195	2a04:4e42:43::323	2001:bb6:6972:e758...	TCP	74	443 → 58260	[ACK] Seq=1 A
58	1.420741	2a04:4e42:400::323	2001:bb6:6972:e758...	TCP	74	443 → 58261	[ACK] Seq=1 A
60	1.420763	2a04:4e42:43::323	2001:bb6:6972:e758...	TCP	1482	443 → 58260	[ACK] Seq=140
61	1.421292	2001:bb6:6972:e758...	2a04:4e42:43::323	TCP	74	58260 → 443	[ACK] Seq=518
62	1.421815	2a04:4e42:43::323	2001:bb6:6972:e758...	TCP	1482	443 → 58260	[ACK] Seq=281

Frame 32: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{D5FB398...}

Ethernet II, Src: IntelCor ce:f9:c8 (5c:e0:c5:ce:f9:c8), Dst: HuaweiTe a2:e6:90 (64:a6:51:a2:e6:90)

Internet Protocol Version 6, Src: 2001:bb6:6972:e758:3584:47cc:8334:2006, Dst: 2a04:4e42:43::323

0110 = Version: 6

.... 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... 0000 0000 0000 0000 = Flow Label: 0x00000

Payload Length: 32

Next Header: TCP (6)

Hop Limit: 64

Source: 2001:bb6:6972:e758:3584:47cc:8334:2006

Destination: 2a04:4e42:43::323

Transmission Control Protocol, Src Port: 58260, Dst Port: 443, Seq: 0, Len: 0

Completed



7. We will look at some of the protocol field information for IPv6. The amount of information in the IPv6 header is much smaller than in the IPv4 header.

The version field is the same i.e. Version 6 and the binary equivalent (0110) beside it.

We can also see the traffic class field which handles traffic prioritization and congestion.

Then we see the flow label which maintains the same packet flows through routers and switches so to help real time applications that need packets to arrive in the same order.

Completed



8. We then have the payload length field which tells us the total size of the packet i.e. 32 bytes.

Next header field and is identifying that the upper layer data portion of this packet is a 6 or TCP.

Hop limit is currently set to 64 hops and once this value decrements to zero, the packet will then be dropped.

Then we have the source IPv6 address, the destination IPv6 address and then we can see that this is a TCP packet, with TCP header information.

Completed

