Video - Sample IPv6 Headers in Wireshark (6 min)

This screenshot shows a packet capture using Wireshark and the network layer information from an IPv6 conversation. Let's take a look at it. In this screenshot, we can see that the highlighted packet is packet number 46 and that the source address up here in the packet list window shows that it is a global unicast IPv6 address. You can see this starting with the 2001:6f8. The destination address is also a global unicast address 2001:6f8:900 and so on. And if we look over in the protocol field, we see that at the upper layers, this is a TCP packet and that it's an attempt to establish an initial communication with an HTTP web server. If we look down in the network layer information area, you can see that the IPv6 information has been expanded. Let's take a look at some of the protocol field information for Internet protocol version 6. First of all, you can see that the amount of information in the IPv6 header is much smaller than in the IPv4 header.

Now, there are some interesting features. For one, you can see that the version field is the same. In this case, it says 6, identifying this packet as IPv6. We can also see the binary 6 here. The next field is the traffic class field. The traffic class field serves the same function as the differentiated services field in an IPv4 packet. It handles traffic prioritization and congestion. The next section you can see is the flow label. The flow label field is a new field for the IPv6 protocol. Its purpose is to maintain the same packet flows through routers and switches, so as to help real-time applications that need packets to arrive in the same order. You can see the next field is the payload length field. This is the same as the total length field in the IPv4 header. This field tells us the total size of the packet-- in this case, 40 bytes. The next header field serves the same purpose as the protocol field for IPv4. You can see that it's identifying that the upper layer data portion of this packet is a 6, or TCP. The hop limit serves the same function as the TTL field in an IPv4 packet. You can see that the hop limit currently is set to 64 hops. Once this decrements to 0, the packet will be dropped. Next, we have the source IPv6 address, the destination IPv6 address, and then, at the upper layer, we can see that this is a TCP packet with TCP header information. Let's take a look at the next screenshot. In the next screenshot, you could see that we've now highlighted packet number 49.

And now we have a connection with this web server. This packet is now a GET request to the web server. If we look down in the expanded Internet protocol version 6 packet details window, we can see that the payload length is a lot larger. We can see below the IPv6 information, the TCP information, and that now there is HTTP protocol information as well within our GET request. This is our GET request to get a webpage. If I go to the next screenshot, the last screenshot shows an ICMP version 6 neighbor solicitation message. If we look up at the window in the highlighted packet here in packet number one, we'll see that the source address this time is not a global unicast IPv6 address, but a link-local address. We can tell that from the fe80 here. We can also see that this link-local address used EUI-64 to resolve the interface identification portion of the address. We can tell that by the ff:fe within the address. The destination address is an ff02 IPv6 address indicating that this is a multicast packet. If we look over at the protocol, we see that it's ICMP version 6, and then information about the packet tells us that this is a neighbor solicitation message for the same device that we were contacting in the earlier screenshots. The function of this packet essentially is similar to an ARP request in IPv4. We need to discover the link-local address of this device, so we send out an ICMP version 6 neighbor solicitation message, multicast it, and we're hoping to get back a link-local address from this neighbor. If we look down in the expanded details window, we can see the version is 6, traffic class, flow label, payload length, which is the entire length of the packet; the next header field, which is like the protocol field of IPv4, indicating a 58, that this is an ICMP version 6 message in the data portion of the packet; the hop limit-- 255 hops. This is similar to the TTL field. And then the source link-local address and the destination multicast IPv6 address. At the bottom, below the IPv6 information, we can see that there's an expandable area specific to the Internet control message protocol version 6.