Computer Networks Lecture

Matthew Bain and Jack Schefer

February 5, 2020

1 Summary

1.1 Topics Covered

- Dial Up Modems
- QAM Modulation
- IPv6
- Network Layer Overview
- Routing Techniques

2 Dial Up Modems

We began today's lecture by examining Dial Up Modems and how they operate. We saw that Dial Up Modems work in the home in the following way:

1. Modem is plugged into telephone line
2. Ethernet cord runs from modem to router
3. Modem is assigned IP Address from ISP (Internet Service Provider)
4. Router will then give IP Addresses to all machines on the network

These networks then communicate with each other in the manner shown in Figure 1.

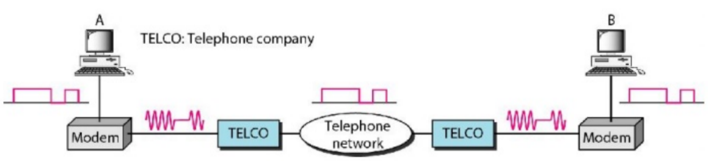

Figure 1: How Modems Communicate

The machines on one network connect to the telephone line through the modem. Then, the packets sent from the first network is modulated and sent along the network. The modulation scheme is **Trelliscoded** modulation. This modulation is a form of QAM modulation. The difference between the two modulation schemes is that one bit is reserved for error checking.

3 QAM Modulation

QAM Modulation, shown in Figure 2, was covered in previous classes, but we went over a short review. This type of modulation takes advantage of amplitude and phase to modulate signals. The number of possible transmitted signals changes based on how accurate the sending and recieving machines can be. For example, a 32-QAM can transmit 5 different bits of information. This is shown in the equation below.

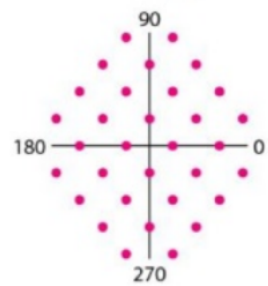

Figure 2: QAM Modulation

$$log_2(QAMValue) = NumberofPossibleBits$$
$$log_2(32) = 5$$

However, in Trelliscoded signals, the last bit is used as error checking, so the available bits for message transmission is actually 4. To calculate the bits per second, you need to know the Baud Rate of the wire and the amount of bits to be transmitted. The bps is just the two multiplied together.

$$NumberofBits = 4$$
$$BaudRate = 2400$$
$$BitsperSecond = 4 * 2400 = 9600bps$$

4 IPv6

4.1 Why Change the Protocol?

There were many reasons that the IPv4 protocol needed a revamping. The most prominent reason is that 32 bits is not sufficient to give an address to all of the machines that will eventually need to be connected to the internet. Others reasons include reducing overhead by modifying the length of the header of the packets, limiting redundancy, and increasing speed of transmission by getting rid of fragmentation.

4.2 New Datagram

The new IPv6 protocol datagram packet is shown in Figure 3 compared to the IPv4 packet discussed in earlier lectures. The main parts of the packet are described below.

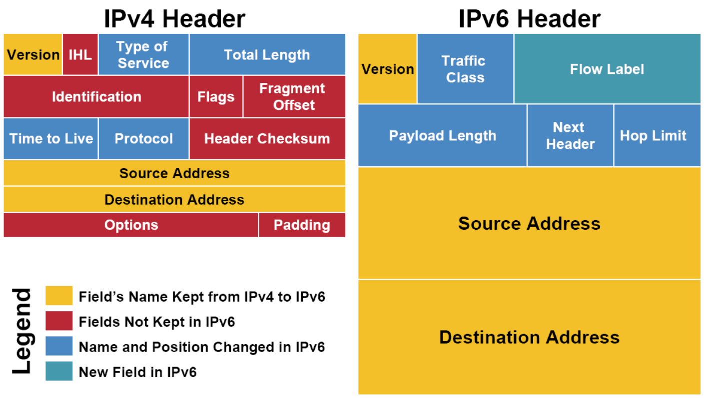

Figure 3: IPv6 Datagram

- Version
  - This is synonomous to the way it was handled in IPv4, except now it holds the number 6.
- Traffic Class (Priority)
  - Similar to TOS field from IPv4, this field lets the router know what message has a higher priority in cases of security, emergency, etc.
- Flow Label
  - A flow is not well defined currently, however this field allows routers to differentiate between types of packets being sent if necessary. This could be used to detect spoofs in the future, but as of now, there isn't really a consensus
- Payload Length
  - Gives the number of bytes in the datagram
- Next Header
  - Identifies the protocol that the contents are delivered (TCP or UDP)
- Hop Limit
  - Decremented by one every time it passes through a router. If reaches 0, it is discarded becuase it is obviously lost.
- Source and Destination Addresses
  - This contains the source address and destination address for the packet
- Data
  - The message being encoded. If the rest of the packet is the envelope, this section of the packet is the letter inside.

4.3 What is Missing?

As seen in the figure, there are parts of the IPv4 packet that are seemingly missing. For instance, there is no more checksum. This is because it is redundant in 99.9% of scenarios. Options are now outside of the header, and there is a new ICMP to account for the loss of fragmentation. If a router cannot handle the packet size, it now sends an error message and asks the packet to be sent again.

4.4 Checksum Review

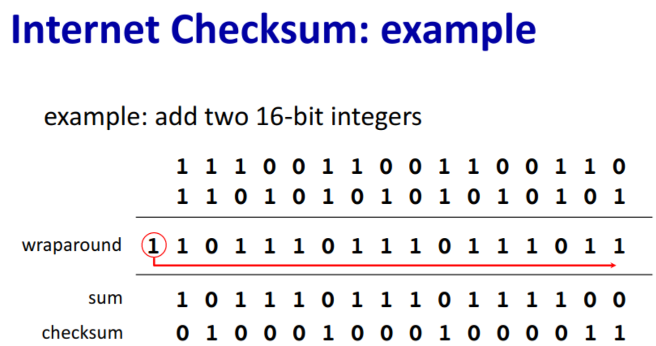

Figure 4: Checksum Review

Even though checksums are absent in IPv6, it is important to know why they were considered to be too much overhead. Take the simple Checksum example in Figure 4. The two integers are added together, then their sum is added to the wraparound(carry) bit. Then the resulting sum's bits are flipped to achieve the final checksum value. This value is sent along with the data packet, and the checksum is XOR with the sum when calculated on the receiving end. If every bit is a 1 after the XOR, the packet was delivered successfully.

4.5 How to Transition from IPv4 to IPv6

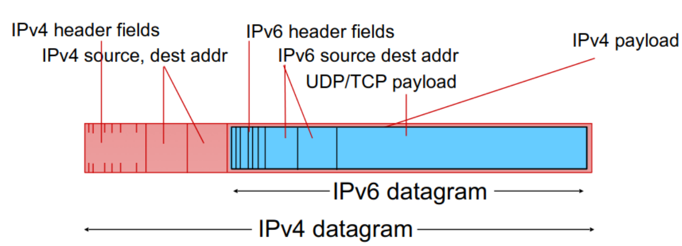

Figure 5: Tunneling

There are two main ideas for transition from IPv4 to IPv6. The first is the idea of the dual stack approach, which we did not discuss very much in lecture. Routers following this approach are viable IPv4 and IPv6 Routers. They have separate IP addresses, and can function wholly as both. This is slightly impractical since the address space on IPv4 is dwindling. The more common method is **tunneling**, where the IPv6 router will send the entire packet inside an IPv4 packet if it is forwarding to an IPv4 router. This is shown in Figure 5. The IPv6 packet is stuffed inside the data section of the IPv4 packet, like an envelope.

5 Network Layer Overview

The network layer can be though of as two different, co-equal planes. The **Data Plane** and the **Control Plane**. The data plane is low level and contains the forwarding table inside the router. The Control plane is high lever, and determines the most optimal path from router to router. In other words, the data plane handles **forwarding**, moving a packet through one signle exchange, and **routing**, moving the packet along the entire network topology.

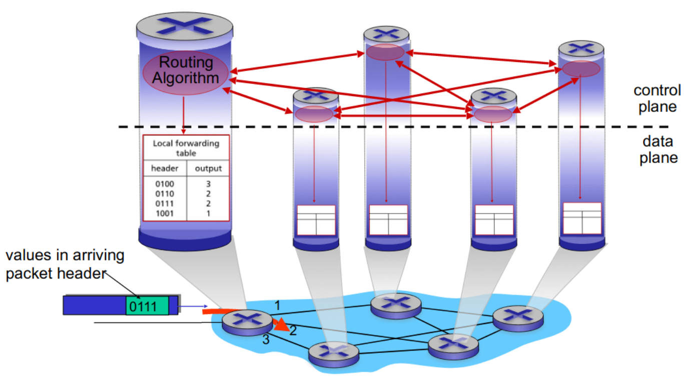

Figure 6: Data Plane vs. Control Plane

6 Routing Techniques

The main idea for routers is that they receive information in the form of packets, detwrmine where the packet needs to go, and sends it on its way. It operates mainly in the data plane.

forwarding table

Destination Address Range	Link Interface
11001000 00010111 00010000 00000000 through 11001000 00010111 00010111 11111111	0
11001000 00010111 00011000 00000000 through 11001000 00010111 00011000 11111111	1
11001000 00010111 00011000 00000000 through 11001000 00010111 00011111 11111111	2
otherwise	3

Figure 7: Forwarding Table

Inside the router is a forwarding table like that shown in Figure 7. Routers analyze the destination address and sends it along the path using **longest prefix matching**. When looking for a forwarding table entry, the router uses the longest address prefix that matches a part in the table.