CS4457 Lecture 7

Phillip Phan (pp5fb), Nikilesh Subramaniam (ns4bb)

February 4, 2020

Contents

1 QAM Modulation

Quadrature amplitude modulation (QAM) Modulation uses amplitude and phase to modulate a signal by using two modulated carrier signals shifted in phase by 90 degrees (they are orthogonal), which are added together to be transmitted. For 32-QAM, there are $\log_2(32) = 5$ bits that can be transmitted as information. Trelliscoded Modulation is QAM Modulation with an extra redundant bit to check for errors. Using 32-QAM with Trelliscoded modulation would only have 4 bits of information to transmit due to the redundant bit. For a baud rate of 2400, Trelliscoded modulation would yield $4 * 2400 = 9600$ bits per second (bps).

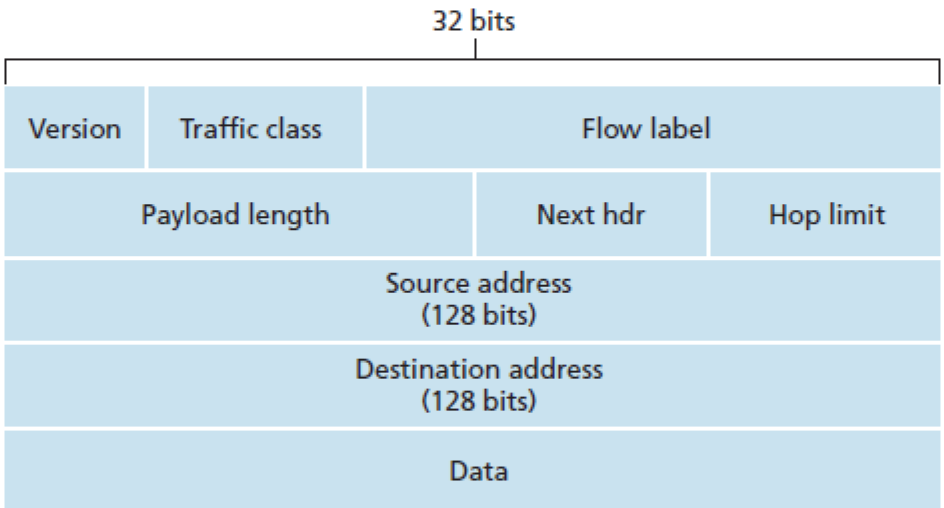
2 IPv6

2.1 Motivation Behind IPv6

There were many inherent problems with IPv4 such as how there were only 32 bits or $2^{32} = 4,294,967,296$ unique addresses that are available to give to various online devices. IPv6 increased the address space to instead allow 128 bits. IPv6 also decreased the amount of processing overhead compared to IPv4 with an improved header structure, and does not allow fragmentation, which prevents fragmentation attacks.

2.2 IPv6 Datagram

The IPv6 datagram packet structure is shown below.



The following list describe each of the fields in the IPv6 datagram.

- Version (4-bits) is the IP version number, which is 6 in Ipv6.
- Traffic Class/Priority (8-bits) is the class or priority of the IPv6 packet, similar to the service field in an IPv4 packet. This allows routers to handle traffic based on priority.
- Flow Label (20-bits) is used to help differentiate packets and see if they belong to the same flow. Flow is not really well defined as of yet.
- Payload Length (16-bits) tells the router the total size of the IPv6 packet in bytes.
- Next Header (8-bits) indicates the type of extension header that follows the IPv6 header such as TCP or UDP.
- Hop Limit (8-bits) is the same as TTL in IPv4 packets, which indicates the maximum amount of intermediate nodes the IPv6 packet is allowed to travel through. This value is decremented by one for each node that forwards the packet, and the IPv6 packet is discarded if the Hop Limit reaches 0.
- Source Address (128-bits) is the IPv6 address of the original source of the packet.
- Destination Address (128-bits) is the IPv6 address of the final destination. This information is used by intermediate nodes to help correctly route the packet.
- Data is the content that is being transmitted using the IPv6 protocol.

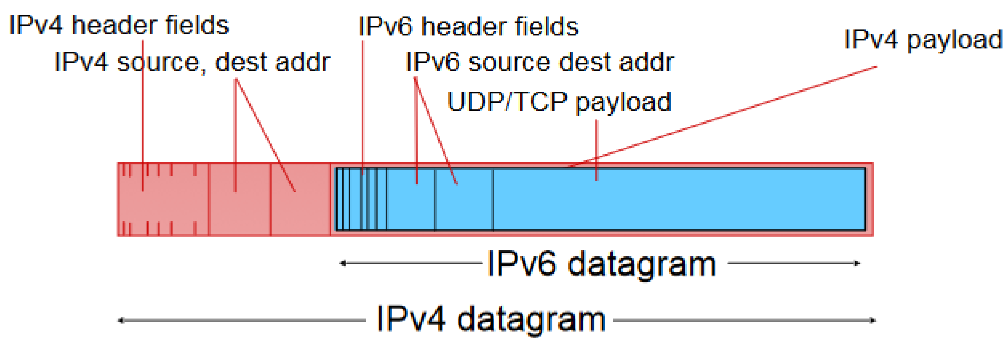
2.3 Other IPv6 Changes

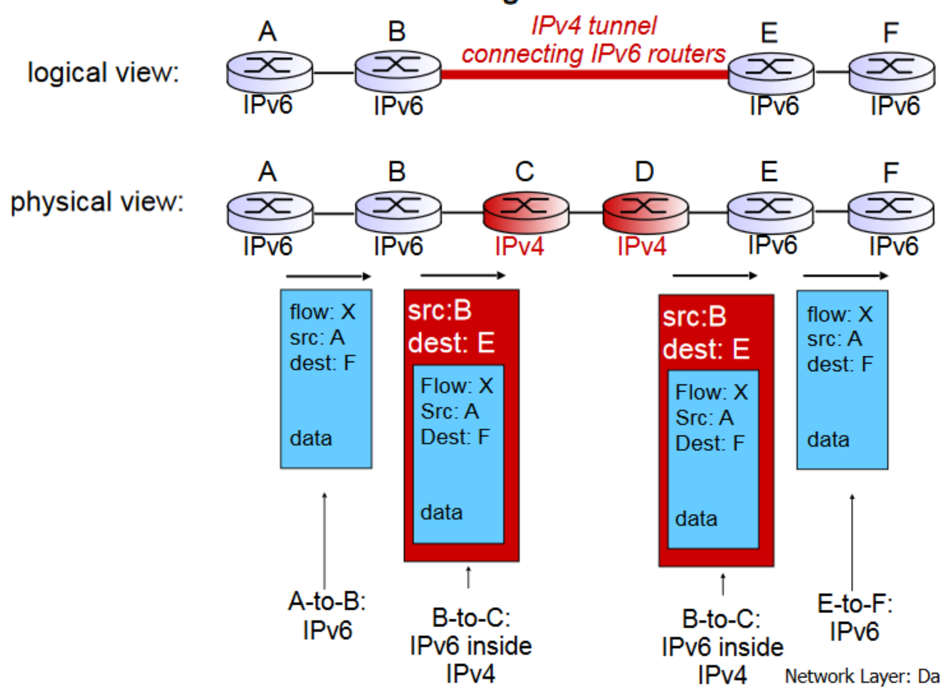
Others changes from IPv4 include the following:

- Checksum being removed to reduce the processing time at each hop.
- Options were moved to be the Next Header field, which is outside the header.
- ICMPv6 is a new version of ICMP that include more message types like "Packet Too Big", and added multicast group management functions.

2.4 Transitioning from IPv4 to IPv6

Since it is logistically impossible to upgrade all routers at the same time to use the IPv6 protocol, tunneling was designed to allow IPv6 and IPv4 to coexist. Tunneling involves having the IPv6 datagram carried as a payload in a IPv4 datagram to transmit with IPv4 routers. This is illustrated in the following two figures.





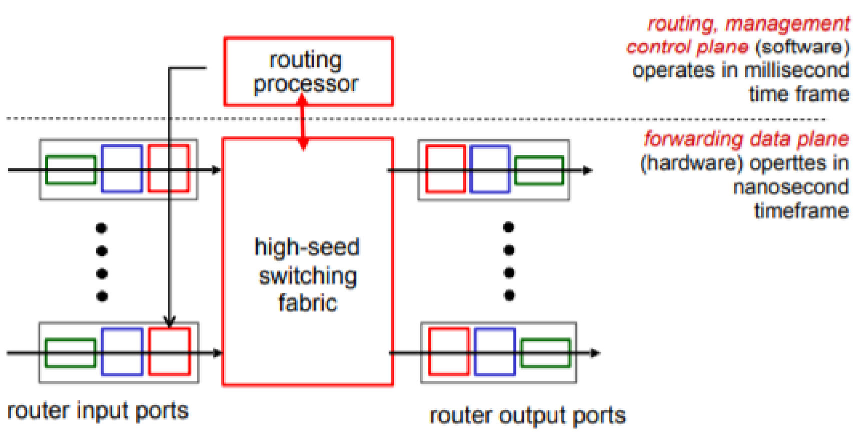
3 Network Layer Overview

The network layer is the layer responsible for transporting segments from the sending side to the receiving side. At the sending side, the segments are encapsulated into datagrams before being sent out. On the receiving side, the segments are delivered to the transport layer. The network layer is present at every host/router. Routers examine header fields in all IP datagrams passing through the router.

The network layer has two main functions:

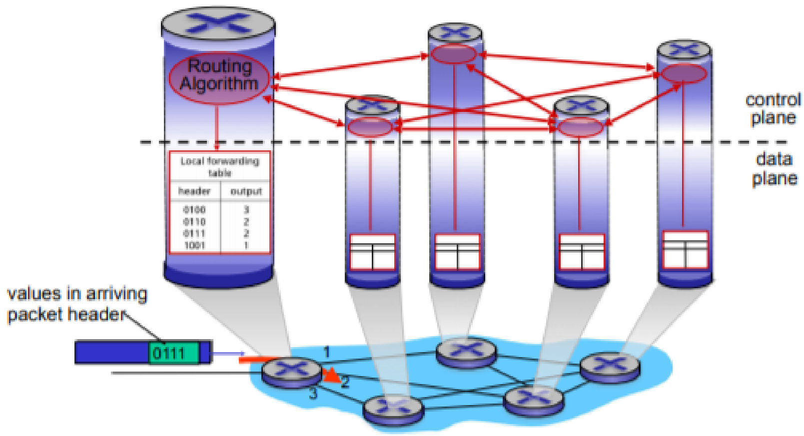
- Forwarding: Move packets from router's input to appropriate router output.
- Routing: Determine the route to be taken by a packet from a source to the destination

The data plane of the network layer handles forwarding. There is a data plane on each router that determines how an arriving datagram is forwarded to an output port. The control plane is network-wide logic that determines the route in which a datagram will be sent. There are two control-plane approaches: traditional routing algorithms in routers and software-defined networks implemented in remote servers.

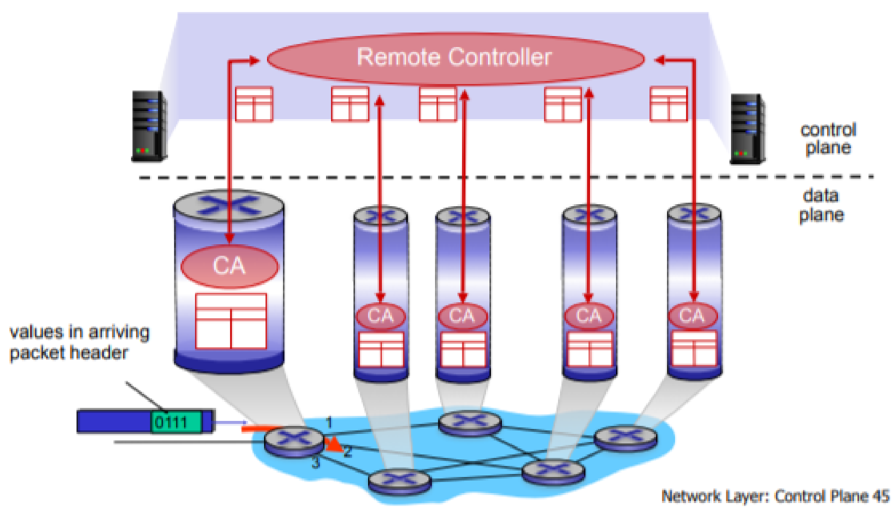


4 Routing

The first control plane approach for routing is implemented on a per-router basis. With this approach, each router has a routing algorithm and the routing algorithm creates a forwarding table used in the data plane.

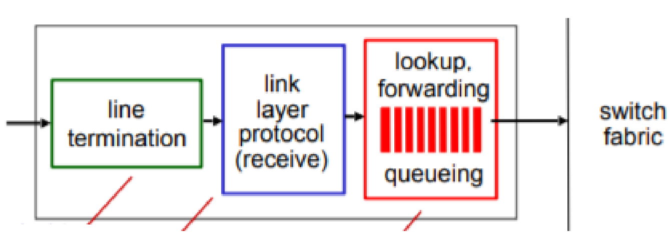


The second control plane approach for routing is by having a locally centralized control plane. In this approach, a remote controller gives forwarding table to each router.



5 Forwarding

For the forwarding function, the data plane figures out how to move packets from the routers input ports to its outputs ports. At the input port, there is the line termination (physical layer), link layer protocol, and the lookup forwarding queue. The output port is found by using the lookup table and the input's header. A queue is used if datagrams arrive too quickly.



In destination based forwarding, the forward is only based on IP address. An example of a forwarding table is shown below. Longest prefix matching is used to quickly figure out which range of IP addresses that the input is in.

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

To quickly perform longest prefix matching, ternary content addressable memories (TCAMs) are often used. They can retrieve the match in one clock cycle regardless of table size.