COMPSCI 630 Systems **Spring 2017**

Lecture 9: Networking

Lecturer: Emery Berger *Scribe(s): Andrew Danise, Jayanth Hegde*

SCRIBE

9.1 LAN Architecture

We reviewed point-to-point, ring, and daisy chain networks. Our discussion focused on how the number of connections used in these networks provide a tradeoff between fault tolerance and network cost.

Early network communication between computer systems was through point-to-point full connections. This requires a lot of wiring. Thus, several network topologies are used to connect all systems in a network. These topologies do not require all systems to be connected to each other but as a trade-off may cause partition when a main connection such as a bus is broken.

Some example topologies: Mesh (fully connected same as the naive connection topology described above), Ring, Daisy chain, Star, Bus or backbone, Tree etc.

9.1.1 Partition Tolerance

We used partition tolerance as a metric to describe the fault tolerance of a network. Partition tolerance is the minimum number of failures a network can sustain before some portion of the network can no longer communicate with another portion.

9.1.2 Point to Point

In a point to point network, each system is directly connected to every other system in the network. Given a network with N nodes, the number of connections in the network is $\frac{N(N-1)}{2}$. This network provides the strongest possible fault tolerance without redundant connections. It has a partition tolerance of N.

9.1.3 Ring

In a ring network, each system is directly connected to two other systems in the network. Given a network with N nodes, the number of connections in the network is N. This network provides weak fault tolerance. It has a partition tolerance of 2.

9.1.4 Daisy Chain

A daisy chain network is similar to a ring network except one the connections is removed. Given a network with N nodes, this topology requires only $N - 1$ connections. The downside is that it has extremely poor fault tolerance. It has a partition tolerance of 1.

9.2 Internet Protocols

We reviewed the UDP and TCP internet protocols.

9.2.1 UDP

UDP or User Datagram Protocol is a simple protocol for transmitting data over a network. It does not try to provide any guarantees about data sent over the network. It is an unreliable protocol meaning it does not guarantee that data actually arrives at its destination. It is also an out of order protocol which means that data can arrive at the destination in a different order than the order it was sent in. The UDP protocol is useful for applications where data is only useful for a small window of time. One example is streaming video. While streaming video, you will not notice if a single frame of the video is dropped as long as most arrive on time.

9.2.2 TCP

TCP or Transmission Control Protocol is a packet based protocol designed to provide reliable transmission of data over a network. In TCP, each packet pecifies the transmission of a single payload of data. Every packet is composed of two parts: a header and a payload. The header contains metadata required to reliably send the packet over the network including the sender, the recipient, the number of the packet, and a checksum to verify the data was sent correctly. The payload is the data being sent. In the TCP protocol, the sender sends a packet to the receiver. If the receiver gets the packet it uses the checksum in the packet header to verify the information. If everything checks out, then the receiver sends an ACK back to the sender. If everything does not check out, then the receiver sends a NACK back to the sender, informing the sender that it needs to resend the data. It is also possible that packets may never reach the receiver (or sender) in which case the sender will retry the message after some timeout has elapsed.

9.3 Packet switching and Virtual Circuits

Method of communication in internet: In a network, communication between two systems occurs through passing of packets. This is referred to as packet switching.

Packet switching in a virtual circuit: A virtual circuit is an abstract circuit established in a network for the purpose of communication. A packet follows a particular path defined by the circuit in this type of communication. This allows packets to reach reliably in an order. TCP is an example of a protocol that uses this type of communication. However, virtual circuit violates the goal of fault tolerance.

Also, virtual circuits do not provide anonymity and security. But it must be remembered that these were not original goals of Internet design.

Original goals of Internet design: Building a resilient, cost-effective communication system for military.

There is also a concept of accountability(tracking the load on our system created by foreign entities). This handled by switches.

An alternative method of communication is to use datagrams. These are used by protocols such as UDP. This method does not guarantee ordered delivery of packets but it guarantees speedy delivery of packets to destination. At the destination, packets are ordered. This is necessary when real time service is required.

9.4 Packet Structure

Consists of a header that contains sender and reciever addresses, sequence number(for TCP and other connection-oriented protocols) and a data payload.

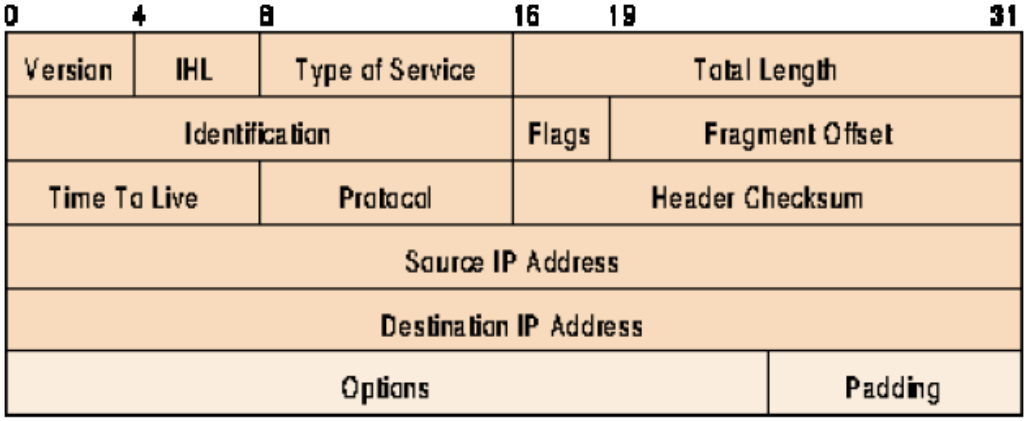

Figure 9.1: IP Header

Typically size of packets ranges from 100 to 1536 bytes.

Fatesharing: States of a communication are stored only at the end points of a communication. This implies that the connecting devices do not have to deal with any of the actual contents of packets. This simplifies the design of network. Thus, connection shares it's fate with the two devices it connects. This is referred to as fate sharing. This is the type of architecture proposed by the end-to-end argument for network design.

9.5 Packet Loss/Corruption

We discussed two causes of packet loss: congestion and network partitions. We also reviewed some causes of packet corruption.

9.5.1 Congestion

When a node in a network does not have the processing power to handle the volume of packets it receives it simply discards excess packets.

9.5.2 Network Partition

When power loss or a hardware/software failure causes a switch to shutdown, any packets the switch was currently processing are discarded.

9.5.3 Packet Corruption

Packet corruption can occur due to software or hardware error which causes the packet data to change. Another cause of packet corruption is electrical charge corruption. This occurs when radiation flips bits of data in transit or while it is store at a node in the network.

9.6 A brief description of working of SMS

SMSes are limited text messages for cellphones. The messages are limited to 160 characters since this is a service piggybacked on an already existing communication method between a tower and a cellphone. Packets already in used for alerting a phone about signal reception strength and incoming calls was used for SMS.