Week 9: Local Area Networks Packets, Frames and Topologies

Comer Chapter 13

- Packet switching forms the basis of the Internet. Uses statistical multiplexing (multiple sources compete for use of shared media)
    - Arbitrary, asynchronous communication
    - No setup required before communication begins
    - Performance varies due to statistical multiplexing among packets
- Categories of networks: LAN (local area network), MAN (metropolitan area network), WAN (wide area network)
- IEEE standards for LANs focus on data link and physical layers
- LAN topologies: bus, ring, star, mesh
    - Bus: single cable to which computers attach. Only one computer can send a signal at a time
    - Ring: computers connected in a closed loop. Can continue operation if some computers are disconnected
    - Star: all computers attach to a central point
    - Mesh: direct connections between each pair of computers. Very expensive.
- MAC addresses contain organizationally unique identifiers (OUI) and network interface controller specific values (NIC)
- Each frame corresponds to a packet. Frames have headers with metadata and payload that contains data being sent

Comer Chapter 14

- IEEE MAC layer has protocols that control access to a shared medium
- Controlled access protocols: distributed version of statistical multiplexing
    - Polling: central controller checks if stations are ready to send packet
    - Reservation: stations declare when they are ready
    - Token passing: passes control message among stations
- Random access protocols: stations contend for access
    - ALOHA: not used in real networks
    - CSMA/CD: collision detection, basis for original Ethernet
    - CSMA/CA: collision avoidance, basis for Wifi networks

Week 10: Datagrams - Structure, Transmission, and Routing

Comer Chapter 22

- "IP datagram" refers to an Internet packet
- General format: header followed by a payload (data area)
- Size of datagram varies and makes IP adaptable to different applications

- IPv4 header has fields with fixed size. IPv6 header is twice as large and contains less information. Most space is for source address and destination address
- Forwarding an IP datagram: IP router uses forwarding table (set of entries that specify a destination and the next hop used to reach that destination)
- Best effort delivery: IP will make best effort to deliver datagram but does not guarantee to handle all problems (datagram duplication, delayed or out of order delivery, corruption of data, datagram loss)
- Encapsulation: entire datagram placed in payload area of frame for transmitting across physical network that does not understand the datagram format

Comer Chapter 23

- 4 key support technologies: address binding, error reporting, bootstrapping, address translation
- ICMP is a companion error reporting mechanism used by routers when datagrams cannot be delivered. ICMP messages are sent to the original source of the datagram.
- DHCP allows host to get necessary information with a single request (IPv4 address, address of default router, address of name server)
- NAT allows site to have multiple computers using the internet through one IPv4 address

Week 11: TCP and UDP Protocols deeper dive

Comer Chapter 24 - UDP: Datagram Transport Service

- The TCP/IP suite contains two major transport protocols the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP)
- UDP is described as a thin protocol layer that provides applications with the ability to send and receive IP datagrams
- UDP provides an end to end service which allows an application program to both send and receive messages where each travels in a separate datagram
- UDP is connectionless meaning that an application can send data at any time and UDP doesn’t transmit any packets besides those that carry user data
- With UDP sending large messages leads to less efficiency due to fragmentation; this is because if a UDP message is larger than the network MTU, then IP will fragment the resulting datagram which reduces efficiency
- A UDP uses best effort delivery semantics meaning that a message could be lost, duplicated, delayed or corrupted, so it’s best for applications that can tolerate delivery errors
- UDP offers four styles of interactions which are: one to one, one to many, many to one, and many to many
- Each UDP message is called a user datagram and is made up of two parts a short header that specifies the sending and receiving applications, and second a payload that carries data being sent

- UDP requires two levels of encapsulation with each message being encapsulated in an IP datagram for transmission across the Internet and the datagram is encapsulated in a frame for transmission across an individual network.

Comer Chapter 25: TCP Reliable Transport Service

- The Transmission Control Protocol (TCP) is a transport layer protocol that provides reliability
- TCP's services offer seven major features which are connection orientation, point to point communication, complete reliability, full duplex communication, stream interface, reliable connection startup and graceful connection shutdown
- Once TCP is requested to establish a connection an application can then receive or send data through it, and TCP guarantees the data's delivery without duplication
- All TCP messages which are sent from one computer to another use the TCP segment format with each segment traveling in an IP datagram
- TCP has a checksum in each segment and it'll retransmit any message that may be lost

Week 12: LAN Equipment

Comer Chapter 15: Wired Lan Technology

- Ethernet has become the standard for wired LANs, the ethernet frame itself starts with a 14 byte header and contains the 48 bit destination address, 48 bit source address, and 16 bit type field
- During the creation of a frame a sender would specify the type and a recipient uses the type to determine which module should process the frame
- There have been three major versions of Ethernet wiring which are thicknet, thinnet and the last version replaces the shared cable with an electronic device called a hub or switch
- The first twisted pair technology operated at 10 Mbps and was designated 10BaseT, with there being a version operating at 100 Mbps and being known as Fast Ethernet, another version known as Gigabit Ethernet operates at 1 Gpbs
- The hardware for higher speeds of Ethernet automatically senses when a low speed device is connected and reduces the speed as required.

Comer Chapter 17: Repeaters, Bridges and Switches

- A max length specification is a part of LAN technology and LAN hardware won't work correctly over wires that exceed the bound
- A pair of fiber modems and optical fibers can be used to provide a connection between a computer and a remote LAN
- A repeater is an analog device used to spread LAN signals over long distances
- A bridge itself is a digital device that connects two LAn segments and transfers packets between them
- The bridge examines MAC addresses in the header of each frame and learns the location of each computer attached to each segment in order to not forward frames that are sent to the computer from other computers on the same segment

- Ethernet switches connect multiple computers and forwards frames among them and the main advantage they have over a hub is that they can transfer multiple packets at the same time as long as one packet is destined for a given output port
- The VLAN switch allows a manager to configure a switch to act like a set of independent switches

Week 13: Wireless Networking

- Wi-Fi has many proven capabilities, given that it has a wider range and extensive connection features
    - Cellular technology such as 4G and 5G are considered as wireless networks
- Different variations of Wi-Fi are differentiated by distance, speed and frequency band
- Encrypted from WEP-WPA2
- Wireless networking presents us with many groundbreaking innovations, such as autonomous vehicles, advanced medicine, etc.
- Bridging is what connects Wireless and wired systems
- Higher frequencies equals shorter wavelengths
    - The higher the frequency, the larger the bandwidth
    - Drawback is that they travel a shorter amount of distance
- Personal Area Networks (PANs) Are made for the purpose of communication over small distances
    - Bluetooth and infrared systems are considered as PANs

Week 14: Security: VPNs, Packet filtering

Comer Chapter 29: Network Security

- Criminal exploits and attacks
    - **Phishing**: Masquerading as a site or a pretending to be a person in order to obtain personal information
    - **Misrepresentation**: Making false claims about goods or services or delivering fake or inferior products
    - **Scams**: Various forms of trickery intended to deceive individuals into investing money or unknowingly albeit in a crime.
    - **Denial of Service:** Intentionally blocking an internet site to prevent or hinder business activities of commerce.
    - **Loss of Control:** An intruder gains control of a user's computer, phone, or other device to commit crimes
    - **Loss of Data:** Loss of intellectual property or other valuable proprietary business information.
- Techniques used to exploit network technologies
    - **Wiretapping**: Making a copy of packets as they traverse in a network to obtain information.

- **Replaying**: Capturing packets from a previous authenticated session and resending it to a different conversation to gain unauthorized access.
- **Buffer Overflow**: Sending more data than a receiver expects in order to store values in variables beyond the buffer.
- **Address Spoofing**: Faking the IP source address in a packet to trick a receiver into processing the packet
- **Name Spoofing**: Using a misspelling of a well-known name or poisoning a name server with an incorrect binding.
- **DoS (Denial of Service) and DDoS (Distributed Denial of Service)**: Flooding a site with packets to prevent the site from successfully conducting normal business.
    - **DDoS (Distributed Denial of Service)**: The usage of multiple computers or devices from around the world to make a coordinated attempt to disrupt a site's normal activities.
- **Phishing**:
- **SYN Flood**: Sending a stream of random TCP SYN segments to exhaust a receiver's set of TCP connections.
- **Password Breaking**: Automated systems that guess a password or a decryption key or to gain unauthorized access.
- **Port Scanning**: Attempting to connect to each possible protocol port on a host to find potential vulnerabilities.
- **Packet Interception**: Capturing and modifying packets destined for another computer in order to get it to respond differently
    - **Another Definition**: Removing a packet from the Internet which allows substitution and man-in-the middle attacks.

<u>3 Multiple Choice Questions:</u>

1) Match the following security technology techniques with their purpose
    - Hashing: **Correct Answer: d**
    - Encryption: **Correct Answer: c**
    - Digital Signatures: **Correct Answer: e**
    - Digital Certificates: **Correct Answer: f**
    - Firewalls: **Correct Answer: a**
    - Intrusion Detection Systems: **Correct Answer: a**
    - VPNs: **Correct Answer: b**

    a) Site Integrity
    b) Data Confidentiality
    c) Privacy

d) Data Integrity
e) Message Authentication
f) Sender Authentication

2) Which network topology is the best for a large organization?
   a. Ring
   b. Bus
   c. Star
   d. Mesh

3) The four styles of interaction for UDP are: one to one, one to many, many to one, and many to many.
   a. True
   b. False