Unit 1

Slide 1

1. What is a computer network?
   Answer: A computer network is a graph-like structure consisting of end-systems or hosts that are connected via communication links and packet switches. These hosts run applications that generate or receive data in the form of packets. The route or path is the sequence of packet switches and communication links. Computer networks are typically managed by one entity responsible for their configuration and operation. Examples include home networks, enterprise networks, and mobile networks.
2. What are end-systems or hosts in a computer network?
   Answer: End-systems or hosts are devices within a network that run applications generating or receiving data packets. These devices are the source and destination of network communication.
3. Explain what a route or path in a computer network is.
   Answer: A route or path in a computer network is the sequence of packet switches and communication links that data packets traverse to move from a source to a destination.
4. Who typically administers a computer network?
   Answer: A computer network is usually administered by one entity that configures and maintains its operation, ensuring its functionality and security.
5. Give examples of different types of computer networks.
   Answer: Examples of computer networks include home networks, enterprise networks, and mobile networks.
6. What is the internet?
   Answer: The internet is a vast computer network that interconnects billions of computing devices worldwide. It is an interconnected architecture that provides services to distributed applications.
7. Briefly describe the history of the internet.
   Answer: The internet evolved from research projects such as DARPA's ARPANET, which introduced packet-switched networks. Over time, key developments like TCP/IP, Ethernet, DNS, the NSFNET program, IANA, ICANN, RFC, IETF, and IESG played vital roles in shaping the modern internet.
8. Who invented the World Wide Web, and when?
   Answer: Tim Berners-Lee invented the World Wide Web in 1989-90 while working at the MIT Laboratory.
9. Who is credited with the invention of email, and in what year?
   Answer: Ray Tomlinson is credited with the invention of email in 1972 while working at BBN (Bolt, Beranek, and Newman).
10. What is DNS, and who invented it?
    Answer: DNS (Domain Name System) is a system that translates domain names into IP addresses, making it easier to access websites. It was invented by Paul Mockapetris at USC in 1982.
11. What does RFC stand for, and who was its originator?
    Answer: RFC stands for Request for Comments, a formal document from the Internet Engineering Task Force (IETF). It was originated by Stephen Crocker at UCLA in 1969.
12. Explain packet switching and identify its inventor.
    Answer:Packet switching is a method of breaking down data into packets before they are transmitted over a network, allowing for more efficient use of the network. Leonard Kleinrock at UCLA developed the concept in 1961.
13. What is TCP/IP, and who developed it?
    Answer: TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols used to interconnect network devices on the internet. It was developed by Bob Kahn and Vincent Cerf while working at DARPA and SRI during 1972-73.
14. Describe Ethernet and its inventor.
    Answer: Ethernet is a network technology for local area networks (LANs), and it was invented by Bob Metcalfe at Xerox PARC in 1973.
15. Who owns or controls the internet?
    Answer: The internet is owned and controlled by ISPs (Internet Service Providers), which are business entities providing internet access to end-systems for a subscription fee. ISPs maintain points-of-presence (PoPs), which are locations where end-systems connect to the internet.
16. What is a point-of-presence (PoP) in an ISP network?
    Answer: A point-of-presence (PoP) is a location where end-systems connect to an ISP network. It typically contains routers, link layer switches, MPLS, and communication links.
17. Explain the hierarchy of ISPs.
    Answer: The ISP hierarchy includes:
    - Access ISPs: Provide internet access to end-users.
    - Regional ISPs: Provide connectivity to access ISPs and connect to Tier 1 ISPs.
    - Tier 1 ISPs: Operate on a global scale and may have bilateral agreements to share resources.
18. How do ISPs generate revenue?
    Answer: ISPs generate revenue as follows:
    - End users pay access ISPs.
    - Access ISPs pay regional ISPs.
    - Regional ISPs pay Tier 1 ISPs.
    - Content service providers may enter into bilateral agreements with ISPs.
    - ISPs performing peering or multi-homing share revenue based on equipment and resource utilization.
19. What are distributed applications, and how does the internet support them?
    Answer: Distributed applications run independently on different hosts or end systems, exchanging messages over the internet using socket interfaces. The internet supports these applications by providing services like reliability and guaranteed data rates, facilitated by protocols that define message formats and the sequence of actions during transmission and reception.
20. What role do protocols play in the functioning of the internet?
    Answer: Protocols define the format and order of messages exchanged between hosts, as well as the actions taken upon the transmission or receipt of messages. They are crucial in ensuring communication reliability and efficiency across the internet.

Slide 2

1. Explain the concept of a network core. How is it different from access networks?
   Answer: The network core, also known as the backbone network, consists of high-speed routers and links like Gigabit Ethernet and optical fibers. It is the part of the internet composed of high-speed packet switches and communication links. Unlike access networks,

which connect end-users to the internet, the network core is responsible for transporting large volumes of data across long distances between ISPs.

2. Describe the function and significance of multiplexers in the network core.
   Answer: Multiplexers in the network core aggregate traffic from access ISPs and connect them to more distant switches through the backbone network. They play a crucial role in efficiently utilizing the network's capacity by combining multiple data streams into one signal over a shared medium.
3. What are the design challenges in the network core, and how are they addressed?
   Answer: Some of the design challenges in the network core include satisfying delay and reliability constraints, routing, assigning capacity (flow maximization problem), and cost improvement. These are addressed through advanced routing algorithms, robust network architectures, and optimization techniques to ensure efficient data transfer and network reliability.
4. Differentiate between circuit switching and packet switching. Provide examples where each is used.
   Answer: Circuit switching requires a dedicated path or circuit to be established between the source and destination before data transfer, ensuring that resources are reserved for the entire session. It is commonly used in traditional telephony. Packet switching, on the other hand, breaks data into smaller packets that are sent independently over the network without reserving a dedicated path. It is more efficient for bursty traffic and is the basis for the modern internet. An example of packet switching is internet data transmission.
5. Explain how Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM) are used in circuit switching.
   Answer: In TDM, time is divided into frames, and each frame is further divided into slots reserved for transmitting hosts. Each slot ends with a guard time to prevent inter-symbol interference (ISI). In FDM, bandwidth is divided into channels, each reserved for transmitting hosts in a fixed slot time. Channels are separated by a guard band to prevent adjacent channel interference. Both techniques are used to allocate resources in circuit-switched networks.
6. Discuss the importance of redundancy in the network core and its impact on network reliability.
   Answer: Redundancy in the network core is crucial for enhancing network reliability. By incorporating multiple paths between routers and switches, redundancy ensures that if one path fails, data can still be routed through an alternative path, thus preventing network outages and ensuring continuous service availability. This is especially important in high-speed networks where even minor disruptions can lead to significant data loss or delays.
7. Explain the 'store and forward' operation performed by packet switches in the network core. How does this differ from traditional switching methods?
   Answer: The 'store and forward' operation involves storing incoming packets in a buffer at the router or switch until the entire packet is received. Once the packet is completely received, it is then forwarded to the appropriate outgoing link. This method contrasts with traditional switching methods like cut-through switching, where forwarding begins as soon as the destination address is recognized, potentially leading to faster but less reliable transmission.
8. Describe the differences between TDM and FDM in circuit switching and provide examples where each would be preferable.
   Answer: TDM (Time Division Multiplexing) divides time into frames, with each frame further divided into time slots. Each slot is dedicated to a specific communication channel. FDM (Frequency Division Multiplexing) divides bandwidth into different frequency channels, each assigned to a specific communication channel. TDM is preferable in scenarios where timing accuracy is critical, such as in synchronous communication systems. FDM is better suited for analog transmission systems, such as traditional radio broadcasting, where different signals need to occupy different frequency ranges simultaneously.
9. Analyze the challenges of designing a network core to satisfy delay and reliability constraints. What strategies can be used to address these challenges?
   Answer: Designing a network core that satisfies delay and reliability constraints requires careful planning of routing algorithms, resource allocation, and network topology. Challenges include minimizing the time it takes for data to travel across the network and ensuring that data is not lost or corrupted during transmission. Strategies to address these challenges include using low-latency routing paths, implementing error detection and correction protocols, and designing the network with redundant paths and failover mechanisms.
10. Explain the concept of circuit establishment in circuit-switched networks. How does this process ensure data integrity during transmission?
    Answer: Circuit establishment in circuit-switched networks involves setting up a dedicated communication path between the source and destination before data transmission begins. This path remains reserved for the entire duration of the communication session, ensuring that the necessary bandwidth and other resources are available, thus preventing data loss or delay. By guaranteeing that resources are not shared with other transmissions, circuit-switched networks ensure data integrity and consistent quality of service.
11. How long does it take to send a file of 640,000 bits from host A to host B over a circuit-switched network? Assume all links are 1.536 Mbps, each link uses TDM with 24 slots/sec, and the guard time is equal to (1/8)th of the slot time. The end-to-end circuit establishment takes 500 msec.
    Answer: The time can be calculated using the given data about link rate, slot division, and guard time, considering the time required to establish the circuit.
12. How long does it take to send a file of 640,000 bits from host A to host B over a circuit-switched network with an available link rate of 1.536 Mbps, distributed across 10 channels of 200 kHz each, and a guard band of 50 Hz? Assume a 500 msec circuit establishment time.
    Answer: The time can be calculated by considering the available bandwidth per channel, the total link rate, and the circuit establishment time.

Slide 4

13. Explain the importance of dividing the data exchange task between two hosts into smaller sub-tasks. How does this division simplify the communication process
    Answer: The complex task of data exchange between two hosts is divided into smaller sub-tasks to maintain simplicity for network devices by putting the burden on the hosts. This division allows each layer to perform its own unique sub-task, making the entire process manageable and efficient.
14. Describe the role of the Application layer in the TCP/IP protocol suite. What are its primary responsibilities?
    Answer: The Application layer is responsible for generating and receiving data on the hosts. It formats the data into messages according to the application layer protocol. This layer also initiates communication with other processes by sending queries or requests.
15. What are the three basic requirements of a protocol in a communication network, and why are they important?
    Answer: The three basic requirements are Syntax, Semantics, and Timing. Syntax concerns the format of data blocks, Semantics includes control information for coordination and error handling, and Timing involves speed matching and sequencing. These ensure proper communication between peer layers.
16. Explain the difference between the TCP/IP model and the OSI model.

Answer: The TCP/IP model consists of 5 layers (Application, Transport, Network, Link, and Physical), whereas the OSI model has 7 layers. The TCP/IP model resulted from protocol research under ARPANET, while the OSI model was proposed as a standardized protocol architecture.

17. How does the Transport layer ensure proper communication between applications on different hosts?
    Answer: The Transport layer ensures proper communication by providing Quality of Service (QoS) for messages, performing multiplexing at the sender, and demultiplexing at the receiver. It maps each message to the corresponding process and appends a header to create a segment.
18. Discuss the role of the Network layer in the TCP/IP protocol suite. How does it handle data transmission between hosts?
    Answer: The Network layer fragments segments into packets and moves them hop-by-hop, using IP addresses. It discovers the path between the source and destination hosts and appends a new header to each packet, creating a datagram.
19. What is the function of the Link layer in the protocol architecture? How does it handle data transmission over a link?
    Answer: The Link layer is responsible for pushing packets onto a link using link layer protocols. It forwards frames using MAC addresses, appends a new header to create a frame, provides synchronization at the receiver, and checks for errors in the frame.
20. Describe the responsibilities of the Physical layer in data transmission.
    Answer: The Physical layer provides the physical interface between the host and the link, converts binary data into signals, performs modulation and demodulation, and handles the transmission, reception, and filtering of signals.
21. Why is it necessary for the same protocol layers to be implemented in both the sender and receiver hosts?
    Answer: The same protocol layers must be implemented in both hosts to ensure that peer layers can communicate effectively. This allows each layer on the sender side to interact with its counterpart on the receiver side using a common set of protocols.
22. How does multiplexing at the Transport layer contribute to the efficient use of network resources?
    Answer: Multiplexing allows multiple messages from different applications to share the same network resources by mapping each message to the appropriate process. This efficient use of resources helps in managing bandwidth and reducing transmission delays.
23. Explain the concept of fragmentation at the Network layer. Why is it necessary?
    Answer: Fragmentation at the Network layer involves breaking down large segments into smaller packets to facilitate their movement through the network. This is necessary because different network paths may have varying maximum transmission unit (MTU) sizes.
24. What is the purpose of error checking in the Link layer, and how is it performed?
    Answer: Error checking in the Link layer ensures that the data transmitted over a link is free from errors. It is performed by checking the integrity of the frame using techniques like checksums or cyclic redundancy checks (CRC) to detect and possibly correct errors.
25. Compare and contrast the roles of the Network and Transport layers in the TCP/IP model.
    Answer: The Network layer is responsible for packet forwarding, routing, and addressing, while the Transport layer ensures reliable data transfer, multiplexing, and error recovery. The Network layer handles the movement of packets across the network, whereas the Transport layer manages end-to-end communication between applications.
26. Discuss the concept of Quality of Service (QoS) in the Transport layer. How does it impact data transmission?
    Answer: Quality of Service (QoS) in the Transport layer refers to the ability to provide different priority levels to different types of data, ensuring that important or time-sensitive data is transmitted with minimal delay and maximum reliability. This impacts data transmission by managing bandwidth allocation, reducing latency, and improving overall network performance.
27. What challenges might arise when implementing protocols in hardware versus software, and how can they be addressed?
    Answer: Implementing protocols in hardware can lead to faster processing speeds but might lack flexibility. In contrast, software implementations are more flexible but may be slower. These challenges can be addressed by using a hybrid approach, where critical time-sensitive tasks are handled by hardware, and more complex, adaptable tasks are managed by software.