Unit 1: Introduction to Computer Networks

1. **What is a computer network?**
    - A computer network is a collection of interconnected devices that can communicate and share resources.
2. **List the characteristics of computer networks.**
    - Reliability, scalability, speed, security, and cost-effectiveness.
3. **What are the primary applications of computer networks?**
    - Resource sharing, data communication, remote access, collaborative work, and multimedia transmission.
4. **Define PAN, LAN, MAN, and WAN.**
    - PAN (Personal Area Network), LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).
5. **What is internetworking?**
    - The practice of connecting multiple computer networks through the use of gateways or routers.
6. **What are the main types of network topologies?**
    - Star, ring, bus, mesh, and hybrid topologies.
7. **Describe a star topology.**
    - A network topology where each device is connected to a central hub or switch.
8. **What is the difference between a LAN and a WAN?**
    - A LAN covers a small geographic area, while a WAN covers a large geographic area, often connecting multiple LANs.
9. **What are the advantages of a bus topology?**
    - Easy to install and extend, cost-effective.
10. **What are the disadvantages of a ring topology?**

- A single point of failure can disrupt the entire network, and adding or removing devices can be difficult.

11. **Explain the concept of network scalability.**
    - The ability of a network to grow and manage increased demand by adding more resources without sacrificing performance.
12. **What is a mesh topology, and where is it used?**
    - A topology where each device is connected to every other device, used in high-reliability environments.
13. **Define a hybrid topology.**
    - A combination of two or more different types of network topologies.
14. **What is a PAN and its typical use case?**
    - A Personal Area Network, typically used for short-range communication like Bluetooth.
15. **How does a MAN differ from a LAN?**
    - A MAN covers a larger geographic area than a LAN and is typically used to connect multiple LANs within a city.
16. **What role does a router play in a WAN?**
    - Routers connect different LANs within a WAN and manage data traffic between them.
17. **What are the benefits of a star topology?**
    - Easy to install and manage, failure of one device doesn’t affect the others.
18. **What is the primary disadvantage of a bus topology?**
    - If the main cable fails, the entire network goes down.
19. **What are network nodes?**

- Devices or data points on a larger network, such as computers, printers, or servers.

20. **Explain the term 'network architecture.'**
    - The design and structure of a computer network, including its physical and logical layout.

Unit 2: Data Communication

1. **What are the components of data communication?**
   - Sender, receiver, message, medium, and protocol.
2. **What are the key characteristics of data communication?**
   - Delivery, accuracy, timeliness, and jitter.
3. **What are transmission impairments in data communication?**
   - Attenuation, noise, and distortion.
4. **What are the different transmission modes?**
   - Simplex, half-duplex, and full-duplex.
5. **Define a communication protocol.**
   - A set of rules governing data communication between devices.
6. **What is the function of a data communication protocol?**
   - To ensure reliable and accurate data transfer.
7. **What is simplex transmission mode?**
   - A one-way communication mode where data flows in a single direction.
8. **Explain half-duplex transmission mode.**
   - Data transmission where both sender and receiver can transmit, but not simultaneously.
9. **What is full-duplex transmission mode?**

- Simultaneous data transmission in both directions.

10. **What causes attenuation in data communication?**
    - The weakening of a signal over distance.
11. **How can noise affect data communication?**
    - It can introduce errors in the data being transmitted.
12. **What is distortion in data communication?**
    - Changes in the signal form or frequency during transmission.
13. **What is a data link layer protocol?**
    - A protocol that handles communication between adjacent network nodes.
14. **What are the primary functions of a protocol?**
    - Error detection, error correction, flow control, and data encapsulation.
15. **What is protocol layering?**
    - Organizing protocols in a hierarchical fashion, each layer providing services to the layer above.
16. **What is flow control in data communication?**
    - Techniques to control the rate of data transmission between sender and receiver.
17. **What are error detection techniques?**
    - Parity checks, checksums, and cyclic redundancy checks (CRC).
18. **What is the significance of data encapsulation?**
    - It allows different layers to add their headers and trailers to the data being transmitted.
19. **What is the purpose of the transmission medium?**
    - To carry the signal from the sender to the receiver.
20. **What are examples of wired transmission media?**

- Twisted pair cables, coaxial cables, and fiber optic cables.

Unit 3: Network Models

1. **What is a layered network architecture?**
   - A design framework that divides the network communication process into distinct layers.
2. **What are the benefits of a layered architecture?**
   - Simplifies troubleshooting, standardizes network components, and allows interoperability.
3. **What is the OSI reference model?**
   - The Open Systems Interconnection model, a seven-layer framework for network communication.
4. **List the seven layers of the OSI model.**
   - Physical, Data Link, Network, Transport, Session, Presentation, Application.
5. **What is the TCP/IP protocol suite?**
   - A set of protocols used for the Internet and similar networks, organized into four layers.
6. **What are the four layers of the TCP/IP model?**
   - Network Interface, Internet, Transport, Application.
7. **What is the primary function of the Physical layer in OSI?**
   - To transmit raw bit streams over a physical medium.
8. **What does the Data Link layer do in the OSI model?**
   - Provides node-to-node data transfer and error detection/correction.
9. **What is the function of the Network layer in OSI?**
   - Handles routing and forwarding of data packets.

10. **What is the role of the Transport layer in OSI?**
    - Provides reliable data transfer services to the upper layers.
11. **What does the Session layer do in the OSI model?**
    - Manages sessions and controls dialogues between applications.
12. **What is the function of the Presentation layer in OSI?**
    - Translates, encrypts, and compresses data for the Application layer.
13. **What services does the Application layer provide in OSI?**
    - Network services directly to end-users.
14. **How does the Internet layer in TCP/IP function?**
    - Manages addressing, packaging, and routing of data packets.
15. **What protocols operate at the Transport layer of TCP/IP?**
    - TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
16. **What is the role of the Network Interface layer in TCP/IP?**
    - Handles hardware addressing and physical transmission of data.
17. **How do the OSI and TCP/IP models differ?**
    - OSI has seven layers, while TCP/IP has four layers. OSI is a theoretical model, and TCP/IP is more practical.
18. **What are the benefits of the TCP/IP model?**
    - Flexibility, interoperability, and scalability.
19. **What is encapsulation in network models?**
    - The process of adding headers and trailers to data as it moves down the layers.
20. **What is the significance of the Application layer in TCP/IP?**
    - It provides network services directly to user applications.

Unit 4: Physical Layer

1. **What are the services provided by the Physical layer?**
    - Bit-by-bit data transmission, physical connection setup, maintenance, and deactivation.
2. **What is a transmission medium?**
    - The physical path between the transmitter and receiver in a communication system.
3. **List examples of wired transmission media.**
    - Twisted pair cables, coaxial cables, and fiber optic cables.
4. **What are wireless transmission media?**
    - Radio waves, microwaves, and infrared signals.
5. **What is the function of networking devices in the Physical layer?**
    - To facilitate data transmission over physical media.
6. **What is the purpose of a modem?**
    - To modulate and demodulate signals for transmission over telephone lines.
7. **How do twisted pair cables transmit data?**
    - By using pairs of wires twisted together to reduce electromagnetic interference.
8. **What are the advantages of fiber optic cables?**
    - High bandwidth, low attenuation, and immunity to electromagnetic interference.
9. **What is the difference between baseband and broadband transmission?**
    - Baseband uses a single signal, while broadband uses multiple signals over different frequencies.
10. **What is a repeater, and why is it used?**

- A device that regenerates and amplifies signals to extend transmission distance.

11. **What is a hub in networking?**
    - A central device that connects multiple devices in a LAN and broadcasts data to all connected devices.
12. **What is the function of a switch?**
    - To connect devices in a network and use MAC addresses to forward data to the correct device.
13. **How does a router differ from a switch?**
    - A router connects different networks and forwards data based on IP addresses, while a switch operates within a single network using MAC addresses.
14. **What is the purpose of an access point?**
    - To provide wireless connectivity to devices within a network.
15. **What are the benefits of using wireless transmission media?**
    - Flexibility, mobility, and ease of installation.
16. **What are the limitations of wireless transmission media?**
    - Susceptibility to interference, limited range, and potential security issues.
17. **What is signal attenuation?**
    - The reduction in signal strength as it travels through a transmission medium.
18. **What is the significance of signal-to-noise ratio (SNR)?**
    - It measures the quality of a signal in relation to background noise, impacting data transmission quality.
19. **What is multiplexing in data communication?**
    - A technique that combines multiple signals for transmission over a single medium.

20. **What are the types of multiplexing?**
    - Frequency Division Multiplexing (FDM), Time Division Multiplexing (TDM), and Code Division Multiplexing (CDM).

Unit 5: Data Link Layer - Error Detection and Correction

1. **What is error detection in data communication?**
    - Techniques to identify errors in transmitted data.
2. **What is error correction in data communication?**
    - Techniques to correct errors without retransmission.
3. **What is a parity bit?**
    - An additional bit added to data to make the number of 1s either even (even parity) or odd (odd parity).
4. **Explain one-dimensional parity.**
    - A parity bit is added to each byte of data to ensure the total number of 1s is even or odd.
5. **What is two-dimensional parity?**
    - Parity bits are added to both rows and columns of data to detect and correct errors.
6. **How does the Hamming code work?**
    - By adding redundant bits to data, it allows error detection and correction of single-bit errors.
7. **What is a cyclic redundancy check (CRC)?**
    - A method that uses polynomial division to detect errors in data.
8. **What is the purpose of a checksum?**
    - To verify data integrity by calculating a value based on the data content.

9. **How does character stuffing work?**
    - Special characters are added to data to differentiate between data and control information.
10. **What is bit stuffing?**
    - Inserting non-information bits into data to prevent misinterpretation of data patterns.
11. **What is the difference between error detection and error correction?**
    - Error detection identifies errors, while error correction fixes them.
12. **What are the benefits of using CRC for error detection?**
    - High accuracy and efficiency in detecting errors.
13. **What is the limitation of parity checks?**
    - It can only detect odd numbers of errors, not even numbers.
14. **What is the advantage of using Hamming code?**
    - It can detect and correct single-bit errors.
15. **How does two-dimensional parity improve error detection?**
    - It increases the likelihood of detecting multiple-bit errors.
16. **What is the significance of error detection and correction in data communication?**
    - Ensures reliable data transfer and minimizes data corruption.
17. **What is the purpose of redundancy in error correction?**
    - To add extra information that can be used to detect and correct errors.
18. **How does CRC differ from checksum?**
    - CRC uses polynomial division, while checksum uses arithmetic summation.
19. **What is the role of the Data Link layer in error control?**

- To detect and correct errors in data frames transmitted between network nodes.

20. **What are the common methods of error detection and correction?**
    - Parity checks, checksums, CRC, and Hamming code.

Unit 6: Data Link Layer - Flow and Error Control Protocols

1. **What is flow control in data communication?**
   - Techniques to manage the rate of data transmission between sender and receiver.
2. **What is the simplest protocol in data communication?**
   - A protocol that transmits data without any flow or error control mechanisms.
3. **Describe the stop-and-wait protocol.**
   - The sender transmits a frame and waits for an acknowledgment before sending the next frame.
4. **What is stop-and-wait ARQ?**
   - An error control protocol where the sender retransmits a frame if an acknowledgment is not received within a certain time.
5. **Explain go-back-n ARQ.**
   - A protocol where the sender can send multiple frames before needing an acknowledgment, but must retransmit all frames from a lost or erroneous frame.
6. **What is selective repeat ARQ?**
   - A protocol where the sender retransmits only the erroneous frames, rather than all frames after the error.
7. **What is the difference between noiseless and noisy channels?**

- Noiseless channels do not have errors during transmission, while noisy channels do.

8. **How does stop-and-wait protocol handle flow control?**
   - By ensuring the sender waits for an acknowledgment before sending the next frame.
9. **What are the disadvantages of the simplest protocol?**
   - Inefficiency and lack of error control.
10. **How does go-back-n ARQ improve efficiency?**
    - By allowing multiple frames to be sent before waiting for an acknowledgment.
11. **What is the primary advantage of selective repeat ARQ?**
    - It minimizes retransmissions by only resending erroneous frames.
12. **What is a frame in data communication?**
    - A data packet at the Data Link layer.
13. **What is the role of acknowledgment in ARQ protocols?**
    - To inform the sender that the frame was received correctly.
14. **How does stop-and-wait ARQ handle error control?**
    - By retransmitting frames if no acknowledgment is received.
15. **What is the window size in go-back-n ARQ?**
    - The number of frames the sender can transmit without waiting for an acknowledgment.
16. **What is the purpose of sequence numbers in ARQ protocols?**
    - To keep track of transmitted and received frames.
17. **How does selective repeat ARQ handle flow control?**
    - By using a sliding window to manage the number of frames in transit.
18. **What are the benefits of using ARQ protocols?**

  - Improved reliability and error handling.

19. **What is the primary limitation of stop-and-wait protocol?**
    - Low efficiency due to waiting for acknowledgments after each frame.
20. **How do flow and error control protocols contribute to data communication?**
    - They ensure reliable and efficient data transfer between sender and receiver.

Unit 7: Data Link Layer - Medium Access Control Protocols

1. **What is pure ALOHA?**
   - A simple protocol where devices transmit whenever they have data, leading to potential collisions.
2. **How does slotted ALOHA improve upon pure ALOHA?**
   - By dividing time into slots, reducing the chance of collisions.
3. **What is persistent CSMA?**
   - A protocol where a device continuously senses the channel and transmits as soon as it becomes idle.
4. **What is non-persistent CSMA?**
   - A protocol where a device senses the channel, and if it's busy, waits a random amount of time before trying again.
5. **Explain CSMA/CD.**
   - Carrier Sense Multiple Access with Collision Detection, where devices detect collisions and retransmit after a random backoff time.
6. **What is CSMA/CA?**
   - Carrier Sense Multiple Access with Collision Avoidance, used primarily in wireless networks to avoid collisions.
7. **What is the primary difference between CSMA/CD and CSMA/CA?**

  - CSMA/CD detects and resolves collisions, while CSMA/CA tries to avoid collisions.

8. **What are the advantages of slotted ALOHA?**
   - Higher efficiency and reduced collisions compared to pure ALOHA.
9. **What is the main disadvantage of pure ALOHA?**
   - High collision probability, leading to low efficiency.
10. **How does persistent CSMA handle collisions?**
    - By continuously sensing the channel and transmitting immediately after it becomes idle.
11. **What are the benefits of non-persistent CSMA?**
    - Reduced chances of collisions and lower channel utilization.
12. **How does CSMA/CD improve network efficiency?**
    - By detecting collisions and reducing the time wasted on retransmissions.
13. **What is the purpose of the backoff algorithm in CSMA/CD?**
    - To determine the random wait time before retransmitting after a collision.
14. **How does CSMA/CA handle collision avoidance?**
    - By using techniques like Request to Send (RTS) and Clear to Send (CTS) to reserve the channel.
15. **What is the role of the Data Link layer in medium access control?**
    - To manage how data frames are placed onto the physical medium.
16. **What is the primary limitation of slotted ALOHA?**
    - Time synchronization is required for all devices.
17. **How does non-persistent CSMA reduce collisions?**
    - By introducing random wait times before attempting to retransmit.
18. **What are the applications of CSMA/CA?**

- Primarily used in wireless networks, such as Wi-Fi.

19. **What is the efficiency of pure ALOHA?**
    - Approximately 18.4%.
20. **What is the efficiency of slotted ALOHA?**
    - Approximately 36.8%.

Unit 8: Network Layer - Logical Addressing

1. **What is IPv4 addressing?**
   - A 32-bit address scheme used to identify devices on a network.
2. **What is classful addressing?**
   - An addressing method that divides the IP address space into five classes (A, B, C, D, E).
3. **What is classless addressing?**
   - An addressing method that allows for more flexible allocation of IP addresses using CIDR (Classless Inter-Domain Routing).
4. **What is subnetting?**
   - The process of dividing a network into smaller sub-networks to improve management and efficiency.
5. **What is Network Address Translation (NAT)?**
   - A technique that allows multiple devices on a private network to share a single public IP address.
6. **What is IPv6 addressing?**
   - A 128-bit address scheme designed to replace IPv4, offering a larger address space.
7. **What is the Address Resolution Protocol (ARP)?**

- A protocol used to map an IP address to a physical MAC address on a local network.

8. **What is the Reverse Address Resolution Protocol (RARP)?**
   - A protocol used to map a physical MAC address to an IP address.
9. **What are the benefits of IPv6 over IPv4?**
   - Larger address space, improved security features, and better support for mobile devices.
10. **What is CIDR, and how does it work?**
    - Classless Inter-Domain Routing, a method for allocating IP addresses and routing that replaces the classful system.
11. **How does NAT improve network security?**
    - By hiding internal IP addresses from external networks.
12. **What is the purpose of subnet masks?**
    - To differentiate the network and host portions of an IP address.
13. **What is the primary advantage of classless addressing?**
    - Greater flexibility in IP address allocation and more efficient use of the address space.
14. **What are private IP addresses?**
    - IP addresses reserved for use within private networks, not routable on the public Internet.
15. **How does ARP work?**
    - By broadcasting a request for the MAC address associated with a known IP address on the local network.
16. **What is the significance of the loopback address in IPv4?**
    - The address 127.0.0.1, used to test network interfaces on a local machine.

17. **What is the difference between static and dynamic IP addressing?**
    - Static IP addresses are manually assigned, while dynamic IP addresses are assigned automatically by a DHCP server.
18. **What is the role of the network layer in logical addressing?**
    - To provide unique addressing for devices on a network and facilitate routing.
19. **What is the purpose of the IPv6 link-local address?**
    - To allow communication between devices on the same local network segment.
20. **What are the three types of IPv6 addresses?**
    - Unicast, multicast, and anycast.

Unit 9: Network Layer – Routing

1. **What is unicast routing?**
    - Routing that directs data from a single sender to a single receiver.
2. **What are the characteristics of routing?**
    - Path selection, routing table maintenance, and forwarding decisions.
3. **What are the main types of routing algorithms?**
    - Distance vector, link-state, and hybrid algorithms.
4. **What is the difference between distance vector and link-state routing?**
    - Distance vector uses distance metrics to find the shortest path, while link-state uses a complete map of the network.
5. **What is the purpose of routing tables?**
    - To store routes and forwarding information for data packets.
6. **What is the primary advantage of link-state routing?**
    - Faster convergence and more accurate routing decisions.
7. **What is the disadvantage of distance vector routing?**

  - Slower convergence and the possibility of routing loops.

8. **What is broadcast routing?**
   - Routing that sends data from one sender to all possible receivers in the network.
9. **What is multicast routing?**
   - Routing that directs data from one sender to multiple specified receivers.
10. **What is the purpose of the routing algorithm?**
    - To determine the best path for data to travel through the network.
11. **How does the OSPF protocol work?**
    - Open Shortest Path First (OSPF) uses link-state information to make routing decisions.
12. **What is the RIP protocol?**
    - Routing Information Protocol, a distance vector routing protocol using hop count as a metric.
13. **What are the benefits of using EIGRP?**
    - Enhanced Interior Gateway Routing Protocol offers fast convergence and scalability.
14. **What is the significance of routing metrics?**
    - Metrics like hop count, bandwidth, and delay help determine the best path for data.
15. **What is the difference between static and dynamic routing?**
    - Static routing uses manually configured routes, while dynamic routing uses algorithms to adjust routes automatically.
16. **What is the role of the network layer in routing?**
    - To determine the best path for data and forward packets accordingly.

17. **What is a routing loop, and how can it be prevented?**
    - A routing loop occurs when data continuously circles through the network. It can be prevented using techniques like split horizon and hold-down timers.
18. **What is the function of the BGP protocol?**
    - Border Gateway Protocol manages routing between different autonomous systems on the Internet.
19. **How does multicast routing differ from broadcast routing?**
    - Multicast routing sends data to a specific group of receivers, while broadcast routing sends data to all receivers in the network.
20. **What are the challenges of routing in Adhoc networks?**
    - Dynamic topology, limited bandwidth, and energy constraints.

Unit 10: Transport Layer - Protocols

1. **What are the services provided by the transport layer?**
    - Connection establishment, data transfer, flow control, error control, and connection termination.
2. **What is the difference between connection-oriented and connectionless services?**
    - Connection-oriented services establish a connection before data transfer (e.g., TCP), while connectionless services do not (e.g., UDP).
3. **What is the process of connection establishment in the transport layer?**
    - The process of setting up a connection between sender and receiver, typically using a three-way handshake in TCP.
4. **What is connection release in the transport layer?**
    - The process of terminating an established connection.
5. **What is TCP?**

   - Transmission Control Protocol, a connection-oriented protocol that ensures reliable data transfer.

6. **What is UDP?**
   - User Datagram Protocol, a connectionless protocol that provides fast but unreliable data transfer.
7. **What is the three-way handshake in TCP?**
   - A process involving SYN, SYN-ACK, and ACK packets to establish a TCP connection.
8. **What are the benefits of using TCP?**
   - Reliable data transfer, error detection and correction, and flow control.
9. **What are the limitations of UDP?**
   - Lack of reliability, no error correction, and no flow control.
10. **How does the transport layer ensure data integrity?**
    - By using checksums and acknowledgments to detect and correct errors.
11. **What is flow control in TCP?**
    - Techniques like sliding window protocol to manage the rate of data transmission.
12. **What is the purpose of the sliding window protocol?**
    - To allow multiple frames to be sent before needing an acknowledgment, improving efficiency.
13. **What is the significance of port numbers in the transport layer?**
    - To identify specific processes or services on a device.
14. **What is the role of the transport layer in end-to-end communication?**
    - To provide reliable data transfer between end devices.
15. **How does TCP handle retransmissions?**

- By using timeouts and sequence numbers to detect lost packets and retransmit them.

16. **What is the difference between a socket and a port?**
    - A port is a communication endpoint, while a socket is an interface for sending and receiving data on a port.
17. **What are the key features of TCP?**
    - Reliable data transfer, flow control, congestion control, and error detection.
18. **What are the key features of UDP?**
    - Low overhead, fast transmission, and suitable for applications that do not require reliability.
19. **How does the transport layer handle multiplexing and demultiplexing?**
    - By using port numbers to direct data to the correct application process.
20. **What is the significance of the transport layer in the OSI and TCP/IP models?**
    - To provide end-to-end communication and ensure reliable data transfer between devices.

Unit 11: Transport Layer - Congestion Control and QoS

1. **What are the general principles of congestion control?**
    - Techniques to prevent and manage network congestion by regulating data transmission rates.
2. **What is congestion avoidance?**
    - Methods to proactively prevent network congestion before it occurs.
3. **What is congestion prevention?**
    - Policies and mechanisms to ensure network resources are used efficiently to avoid congestion.

4. **What is Quality of Service (QoS)?**
   - Techniques to manage network traffic to ensure the performance of critical applications.
5. **What are the types of network traffic?**
   - Real-time traffic, non-real-time traffic, and best-effort traffic.
6. **What is traffic shaping?**
   - Techniques to control the
7. **What is the purpose of traffic shaping in QoS?**
   - To control the flow of network traffic according to predefined rules and priorities.
8. **Explain the leaky bucket algorithm.**
   - A traffic shaping algorithm that limits the rate at which data can be sent out of a network interface.
9. **How does the token bucket algorithm work?**
   - Tokens are added to a bucket at a fixed rate, and only devices with tokens can transmit data.
10. **What are the characteristics of real-time traffic?**
    - Requires low latency and jitter to maintain quality, such as voice and video streaming.
11. **What is the difference between traffic shaping and traffic policing?**
    - Traffic shaping buffers excess traffic, while traffic policing drops excess traffic.
12. **What is the role of QoS in network management?**
    - To prioritize traffic and allocate network resources to ensure the performance of critical applications.

13. **What are the challenges of implementing QoS in networks?**
    - Compatibility issues, configuration complexity, and resource allocation.
14. **How does the leaky bucket algorithm contribute to congestion control?**
    - By smoothing out bursts of traffic and controlling the rate of transmission.
15. **What is the purpose of traffic prioritization in QoS?**
    - To ensure that critical applications receive preferential treatment over less important traffic.
16. **What are the types of traffic shaping techniques?**
    - Token bucket, leaky bucket, and traffic shaping policies.
17. **How does QoS impact network performance?**
    - It improves the reliability and predictability of network performance for different types of traffic.
18. **What is the significance of jitter in real-time traffic?**
    - Jitter affects the quality of voice and video transmission by causing delays and variations in packet arrival times.
19. **What are the benefits of implementing congestion control mechanisms?**
    - Improved network efficiency, reduced packet loss, and better user experience.
20. **How does QoS support end-to-end communication in networks?**
    - By ensuring that traffic receives appropriate prioritization and resource allocation based on application requirements.

Unit 12: Application Layer - Services and Protocols

1. **What are the services provided by the application layer?**
    - Remote access, file transfer, email services, and web browsing.
2. **What is remote login (TELNET)?**

- A protocol that allows remote access to a host computer over a network.

3. **What is the File Transfer Protocol (FTP)?**
   - A protocol used for transferring files between a client and a server over a network.
4. **What is the Domain Name System (DNS)?**
   - A protocol that translates domain names into IP addresses.
5. **What is the Simple Mail Transfer Protocol (SMTP)?**
   - A protocol used for sending email messages between servers.
6. **What is the Post Office Protocol (POP)?**
   - A protocol used for retrieving email messages from a server to a client.
7. **What is the Internet Message Access Protocol (IMAP)?**
   - A protocol used for accessing and managing email messages on a server.
8. **How does TELNET facilitate remote access?**
   - By establishing a virtual terminal session between a client and a remote host.
9. **What are the security concerns associated with TELNET?**
   - It transmits data in plain text, making it vulnerable to eavesdropping.
10. **How does FTP ensure file transfer security?**
    - By supporting secure FTP (SFTP) and FTPS protocols that encrypt data during transmission.
11. **What is the role of DNS in web browsing?**
    - It translates domain names (e.g., www.example.com) into IP addresses to locate web servers.
12. **How does SMTP facilitate email communication?**
    - By transferring outgoing email from a client to a server and between servers.
13. **What is the purpose of POP in email retrieval?**

- To download and manage email messages from a server to a local client device.

14. **How does IMAP differ from POP?**
    - IMAP allows users to access and manage email messages directly on the server, while POP downloads messages to the client.
15. **What are the benefits of using DNS caching?**
    - Faster domain name resolution and reduced network traffic.
16. **What are the challenges of using FTP in a secure manner?**
    - Requires additional configuration for secure FTP protocols and potential firewall issues.
17. **What is the role of application layer protocols in network communication?**
    - To define communication rules and formats for specific services and applications.
18. **How does DNS load balancing improve web service availability?**
    - By distributing client requests across multiple servers based on IP address resolution.
19. **What are the advantages of using IMAP over POP?**
    - Allows users to access and manage emails from multiple devices without downloading them.
20. **What is the importance of secure email transmission using SMTP protocols?**
    - To prevent unauthorized access and ensure the confidentiality of email communications.

Unit 13: Internet and WWW

1. **What are the basic principles of the Internet?**
   - Decentralized network architecture, packet switching, and global connectivity.
2. **Explain the Hypertext Transfer Protocol (HTTP).**
   - A protocol used for transferring hypertext requests and information on the World Wide Web.
3. **What is the World Wide Web (WWW)?**
   - A system of interlinked hypertext documents accessed via the Internet.
4. **How does IPsec enhance security on the Internet?**
   - By providing authentication and encryption for IP packets.
5. **What is a Virtual Private Network (VPN)?**
   - A secure network connection established over a public network like the Internet.
6. **How does HTTP facilitate client-server communication on the web?**
   - By allowing clients to request web pages and servers to respond with content.
7. **What are the challenges of maintaining data integrity on the Internet?**
   - Data interception, unauthorized access, and malware threats.
8. **How does HTTPS differ from HTTP?**
   - HTTPS encrypts data transmitted between the client and server, providing secure communication.
9. **What role does DNS play in web browsing?**
   - It translates domain names into IP addresses to locate web servers.
10. **What are the benefits of using IPsec in VPNs?**
    - Enhanced security through encryption, authentication, and data integrity verification.

11. **Explain the importance of IP addressing in Internet communication.**
    - IP addresses uniquely identify devices on the Internet and facilitate data routing.
12. **What is the significance of VPN tunnels in secure communications?**
    - They create encrypted paths for data transmission over public networks.
13. **How does DNS resolution affect web browsing performance?**
    - Fast DNS resolution results in quicker access to websites.
14. **What are the security risks associated with HTTP connections?**
    - Data interception, eavesdropping, and man-in-the-middle attacks.
15. **How does IPsec protect against network attacks?**
    - By authenticating and encrypting IP packets to ensure data confidentiality and integrity.
16. **What is the role of IP addressing in VPN tunneling?**
    - To route encrypted data packets between VPN endpoints over the Internet.
17. **What are the advantages of using HTTPS for secure web browsing?**
    - Protection against data tampering, privacy violations, and authentication risks.
18. **How does DNS caching improve Internet performance?**
    - By storing recently accessed DNS information locally to reduce query response times.
19. **What are the challenges of implementing IPsec in large-scale VPN deployments?**
    - Compatibility issues, configuration complexity, and performance overhead.
20. **What is the impact of IPsec on VPN throughput and latency?**
    - IPsec encryption and decryption processes can affect VPN performance, requiring optimization.

Unit 14: Network Security

1. **What are the primary goals of network security?**
   - Confidentiality, integrity, availability, and authenticity of data and resources.
2. **Explain the principles of cryptography in network security.**
   - Encryption, decryption, and key management to secure data during transmission and storage.
3. **How does message integrity ensure data reliability in network communications?**
   - By detecting unauthorized alterations or tampering of data.
4. **What are the techniques for securing email communications?**
   - Encryption (e.g., PGP, S/MIME), digital signatures, and secure email protocols (e.g., SMTPS).
5. **How do firewalls enhance operational security in network environments?**
   - By filtering network traffic based on predefined security rules and policies.
6. **Explain the concept of intrusion detection systems (IDS).**
   - Systems that monitor network traffic for suspicious activity or policy violations.
7. **What are the different types of firewalls?**
   - Packet filtering, stateful inspection, proxy firewalls, and next-generation firewalls.
8. **How does encryption contribute to data security in network communications?**
   - By scrambling data into unreadable format that can only be deciphered with the correct decryption key.
9. **What is the role of access control in network security?**
   - To restrict unauthorized access to network resources based on user credentials and policies.

10. **How does network segmentation improve security posture?**
    - By isolating sensitive network segments from less secure areas to contain potential threats.
11. **Explain the operational benefits of using VPNs for secure remote access.**
    - Employees can securely access corporate networks from remote locations using encrypted tunnels.
12. **What are the challenges of implementing encryption in network environments?**
    - Key management, performance impact, and compatibility with existing systems.
13. **How do digital certificates enhance authentication in network communications?**
    - They validate the identity of communicating parties and establish secure connections.
14. **What are the advantages of using intrusion prevention systems (IPS) over IDS?**
    - IPS can actively block or mitigate detected threats in real-time, whereas IDS only provides alerts.
15. **What are the best practices for securing wireless networks?**
    - Enabling encryption (e.g., WPA2), disabling SSID broadcasting, and using strong passwords.
16. **How does network auditing contribute to security maintenance?**
    - By assessing network configurations, policies, and access controls for compliance and vulnerabilities.
17. **Explain the role of security policies in maintaining network integrity.**
    - They define rules and guidelines for protecting network assets and responding to security incidents.
18. **What are the challenges of securing IoT devices in network environments?**

- Limited resources for security measures, diverse device types, and potential vulnerabilities.

19. **How does penetration testing help identify network security weaknesses?**
    - By simulating real-world attacks to assess the effectiveness of security controls and defenses.
20. **What are the considerations for implementing secure remote access solutions?**
    - Authentication methods, encryption protocols, and monitoring for unauthorized access attempts.