## Review Questions

1. Which protocol's header would a layer 4 device read and process?

    a. IP

    b. TCP

    c. ARP

    d. HTTP

    **Answer**: b. TCP

    **Explanation**: Each device is known by the innermost OSI layer header it reads and processes; **TCP (Transmission Control Protocol)** operates in the transport layer of the OSI model. IP (Internet Protocol) belongs to the network layer of the OSI model. ARP (Address Resolution Protocol) is a layer 2 protocol that works with IPv4 in layer 3. HTTP (Hypertext Transfer Protocol) is an application layer protocol.

2. What field in a TCP segment is used to determine if an arriving data unit exactly matches the data unit sent by the source?

    a. Source port

    b. Acknowledgment number

    c. DiffServ

    d. Checksum

    **Answer**: d. Checksum

    **Explanation**: TCP sends a character string called a **checksum**; TCP on the destination host then generates a similar string. If the two checksums fail to match, the destination host asks the source to retransmit the data. The Source port field indicates the port at the source host. The Acknowledgment number field confirms receipt of data via a return message to the sender. The DiffServ field in an IPv4 header informs routers the level of precedence they should apply when processing the incoming packet.

3. At which OSI layer does IP operate?

    a. Application layer

    b. Transport layer

    c. Network layer

    d. Data link layer

    **Answer**: c. Network layer

    **Explanation**: IP (Internet Protocol) belongs to the **network layer** of the OSI model. It allows data to traverse more than one LAN segment and more than one type of network through a router, which is a network layer device. Data and instructions, known as the payload, are generated by an application running on the source host, and the application layer describes the interface between two applications, each on separate computers. A transport layer protocol, usually either TCP or UDP, adds a header in front of the payload; this header includes a port to identify the receiving application on the destination host. The data link layer encapsulates data in a frame that includes a physical address used to find a node on the local network; common data link layer protocols are Ethernet and Wi-Fi.

4. What is the Internet standard MTU?

   a. 65,535 bytes

   b. 1,522 bytes

   c. 1,500 bytes

   d. 9,198 bytes

   **Answer**: c. 1,500 bytes

   **Explanation**: For Ethernet, the default MTU is **1,500 bytes**, a value that is generally considered the Internet standard. The maximum size of a network layer packet is 65,535 bytes. Ethernet frames on a VLAN (virtual LAN) can have an extra 4-byte field and a maximum frame size of 1,522 bytes. Some special-purpose networks use a proprietary version of Ethernet that allows for a jumbo frame, in which the MTU can be set above 9,000 bytes.

5. Which two protocols manage neighbor discovery processes on IPv4 networks?

   a. ICMP and ARP

   b. IPv4 and IPv6

   c. TCP and UDP

   d. NDP and Ethernet

   **Answer**: a. ICMP and ARP

   **Explanation**: On IPv4 networks, neighbor discovery is managed by **ARP (Address Resolution Protocol)** with help from **ICMP (Internet Control Message Protocol)**. IP (Internet Protocol) versions 4 and 6 specify where data should be delivered and enable TCP/IP to internetwork. TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) include a physical address used to find a node on the local network. NDP (Neighbor Discovery Protocol) eliminates the need for ARP and some ICMP functions in IPv6 networks. Ethernet uses physical addresses to find nodes on the local network.

6. You're getting a duplicate IP address error on your computer and need to figure out what other device on your network is using the IP address 192.168.1.56. What command will show you which MAC address is mapped to that IP address?

   a. telnet 192.168.1.56

   b. tracert 192.168.1.56

   c. arp -a

   d. netstat -n

**Answer**: c. arp -a

**Explanation**: The database of IP-to-MAC address mappings is called an ARP table; to view a workstation's ARP table, enter the command arp -a. The command telnet 192.168.1.56 will attempt to connect to a device on the network at the IP address listed. The command tracert 192.168.1.56 will trace a path from the local node to the node at the listed IP address. The netstat -n command lists current connections on the local device, including IP addresses and ports.

7. What is one advantage offered by VDI over RDS and VNC?

   a. Offers access to multiple OSs in VMs

   b. Supports remote access to mobile devices

   c. Allows multiple users to sign in at once

   d. Provides open source flexibility

   **Answer**: a. Offers access to multiple OSs in VMs

   **Explanation**: VDI (Virtual Desktop Infrastructure) **offers access to VMs running many different OSs**. VNC (Virtual Network Computing) is open source so other companies can develop their own software, and it supports remote access to computers, tablets, and smartphones. RDS (Remote Desktop Services) allows multiple users to access the same virtual or physical Windows Server at one time.

8. Which encryption protocol does GRE use to increase the security of its transmissions?

   a. SSL

   b. SFTP

   c. IPsec

   d. SSH

   **Answer**: c. IPsec

   **Explanation**: GRE (Generic Routing Encapsulation) is a versatile tunneling protocol and, like many tunneling protocols, it's used in conjunction with **IPsec (IP Security)** to increase the security of its transmissions. SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are both methods of encrypting TCP/IP transmissions, such as HTTP, SMTP, LDAP, IMAP, and POP3. SFTP (Secure FTP) is a file-transfer version of SSH (Secure Shell), which is a collection of protocols that performs both authentication and encryption for a remote access session.

9. Which encryption benchmark ensures data is not modified after it's transmitted and before it's received?

   a. Confidentiality

   b. Integrity

    c. Availability

    d. Symmetric

**Answer**: b. Integrity

**Explanation**: **Integrity** ensures data is not modified in the time after the sender transmits it and before the receiver picks it up. Confidentiality ensures data can only be viewed by its intended recipient or at its intended destination. Availability ensures data is available and accessible to the intended recipient when needed. Symmetric key encryption uses the same key during both the encryption and decryption of the data.

10. Which remote file access protocol is an extension of SSH?

    a. SFTP

    b. TFTP

    c. FTPS

    d. HTTPS

    **Answer**: a. SFTP

    **Explanation**: **SFTP (Secure FTP)** is a file-transfer version of SSH that includes encryption and authentication, and it's sometimes inaccurately called FTP over SSH or SSH FTP. TFTP (Trivial FTP) is a simple protocol similar to FTP except that it includes no authentication or security for transferring files. FTPS (FTP Secure or FTP over SSL) provides an added layer of protection for FTP using SSL/TLS that can encrypt both the control and data channels. HTTPS (HTTP Secure) uses SSL/TLS encryption and TCP port 443 rather than port 80.

11. What three characteristics about TCP distinguish it from UDP?

    **Answer**: TCP is connection-oriented, uses sequencing and checksums, and provides flow control.

12. What process is used to establish a TCP connection?

    **Answer**: Three-way handshake

13. What is the difference between dynamic ARP table entries and static ARP table entries?

    **Answer**: Dynamic ARP table entries are created when a client makes an ARP request, whereas static ARP table entries are entered manually using the ARP utility.

14. Which two fields in an Ethernet frame help synchronize device communications but are not counted toward the frame's size?

    **Answer**: Preamble and SFD

15. Explain the key difference between how symmetric encryption works and how asymmetric encryption works.

**Answer**: Symmetric encryption uses the same key during both the encryption and decryption of the data. Asymmetric encryption requires the use of two different keys, one to encrypt and the other to decrypt.

16. Which secured tunneling protocol might be able to cross firewalls where IPsec is blocked?

    **Answer**: OpenVPN

17. When surfing online, you get some strange data on an apparently secure website, and you realize you need to check the legitimacy of the site. What kind of organization issues digital certificates for websites?

    **Answer**: CA (Certificate Authority)

18. What tcpdump command will capture data on the eth0 interface and redirect output to a text file named checkme.txt for further analysis?

    **Answer**: tcpdump -i eth0 -w checkme.txt

19. Which terminal emulation protocol is similar to RDP but is open source?

    **Answer**: VNC (Virtual Network Connection)

20. Which port must be open for RDP traffic to cross a firewall?

    **Answer**: 3389