MCQ regarding Network Security

1. **What is the primary function of a firewall in network security?**
    - **A. To create a wireless network**
    - **B. To monitor and control incoming and outgoing network traffic**
    - **C. To store data securely**
    - **D. To manage network bandwidth**
2. **Which protocol is commonly used to secure web traffic on the internet?**
    - **A. HTTP**
    - **B. FTP**
    - **C. HTTPS**
    - **D. SMTP**
3. **What does VPN stand for?**
    - **A. Virtual Public Network**
    - **B. Virtual Private Network**
    - **C. Virtual Protected Network**
    - **D. Virtual Proxy Network**
4. **Which of the following is a characteristic of a stateful inspection firewall?**
    - **A. It filters packets based only on static information**
    - **B. It tracks the state of active connections**
    - **C. It blocks all incoming traffic by default**
    - **D. It acts as a proxy for web requests**
5. **Which encryption algorithm is commonly used for securing wireless networks under WPA2?**
    - **A. DES**

- **B. RSA**
- **C. AES**
- **D. MD5**

6. **What type of attack involves intercepting and altering communication between two parties?**
   - **A. Denial of Service (DoS)**
   - **B. Phishing**
   - **C. Man-in-the-Middle (MitM)**
   - **D. SQL Injection**
7. **Which layer of the OSI model is responsible for data encryption?**
   - **A. Physical Layer**
   - **B. Data Link Layer**
   - **C. Transport Layer**
   - **D. Presentation Layer**
8. **What is the main purpose of an Intrusion Detection System (IDS)?**
   - **A. To prevent unauthorized access**
   - **B. To detect and alert on suspicious activities**
   - **C. To encrypt network traffic**
   - **D. To manage user authentication**
9. **Which of the following is a commonly used port for HTTPS traffic?**
   - **A. 20**
   - **B. 21**
   - **C. 80**
   - **D. 443**
10. **What is the primary difference between a virus and a worm?**

- **A. A virus requires user action to spread, while a worm can spread autonomously**
- **B. A virus encrypts data, while a worm does not**
- **C. A virus is a type of malware, while a worm is not**
- **D. A virus can spread through email, while a worm cannot**

11. **Which security measure involves converting plaintext data into a coded form to prevent unauthorized access?**
    - **A. Authentication**
    - **B. Encryption**
    - **C. Hashing**
    - **D. Firewalling**
12. **What is the purpose of a digital certificate in network security?**
    - **A. To store user passwords securely**
    - **B. To provide software licenses**
    - **C. To verify the identity of a server or user**
    - **D. To encrypt email messages**
13. **Which attack exploits vulnerabilities in web applications to execute malicious scripts in a user's browser?**
    - **A. Cross-Site Scripting (XSS)**
    - **B. Cross-Site Request Forgery (CSRF)**
    - **C. Buffer Overflow**
    - **D. Directory Traversal**
14. **What does SSL stand for in the context of network security?**

- A. Secure Sockets Layer
- B. Secure Systems Link
- C. Secure Shell Layer
- D. System Security Layer

15. What is the role of a Certificate Authority (CA) in network security?
    - A. To issue digital certificates
    - B. To monitor network traffic
    - C. To manage firewall rules
    - D. To encrypt data transmissions

Answers

1. B. To monitor and control incoming and outgoing network traffic
2. C. HTTPS
3. B. Virtual Private Network
4. B. It tracks the state of active connections
5. C. AES
6. C. Man-in-the-Middle (MitM)
7. D. Presentation Layer
8. B. To detect and alert on suspicious activities
9. D. 443
10. A. A virus requires user action to spread, while a worm can spread autonomously
11. B. Encryption
12. C. To verify the identity of a server or user
13. A. Cross-Site Scripting (XSS)
14. A. Secure Sockets Layer

https://www.sanfoundry.com/computer-fundamentals-questions-answers-network-security-encryption/
https://www.sanfoundry.com/cyber-security-questions-answers-virus-worms/

Transport Layer

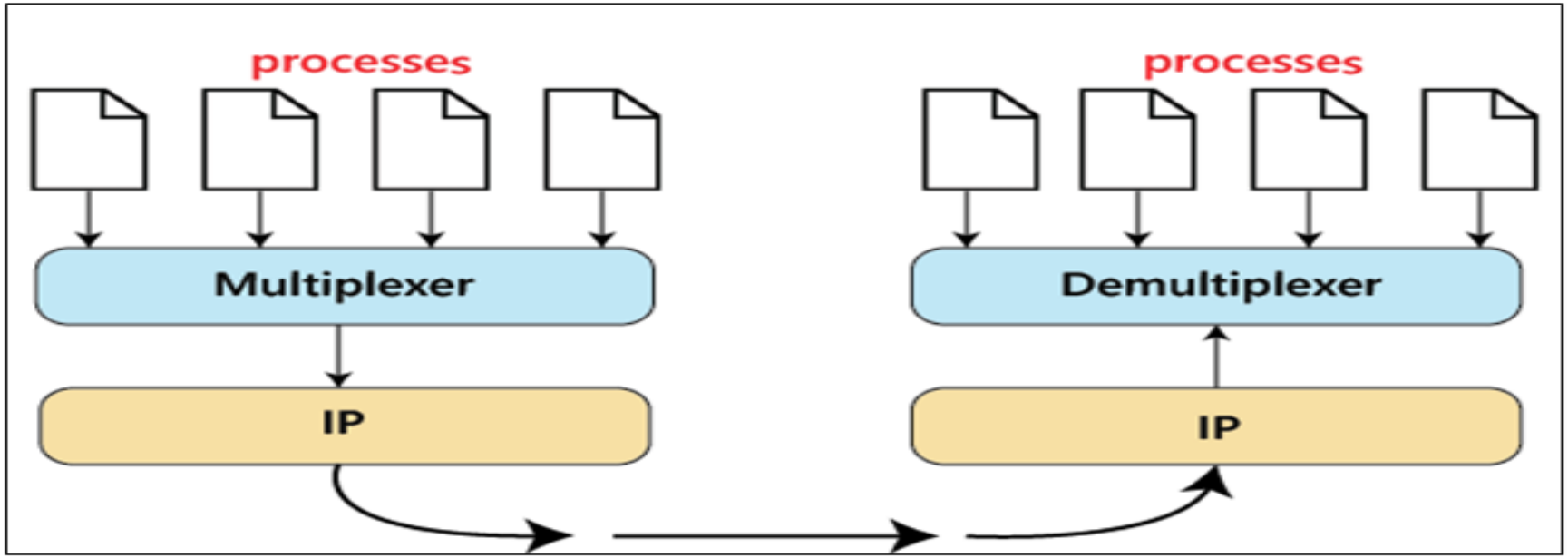
PANA ACADEMY

Services of Transport Layer

Responsibilities of a Transport Layer

- The Process to Process Delivery
- End-to-End Connection between Hosts
- Multiplexing and Demultiplexing
- Congestion Control
- Data integrity and Error correction
- Flow control

Diagram Explaining Process to Process Communication



Process to Process Delivery

TCP VS UDP

TCP	UDP
TCP is a connection-oriented protocol.	UDP is the Connection less protocol.
TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
An acknowledgment segment is present.	No acknowledgment segment.
Sequencing of data is a done in this protocol.	There is no sequencing of data in UDP.
TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.
TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
TCP is used by HTTP, HTTPs, FTP , SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP,SNMP, RIP, and VoIP.

Port and Socket

A port is a logical construct assigned to network processes so that they can be identified within the system.

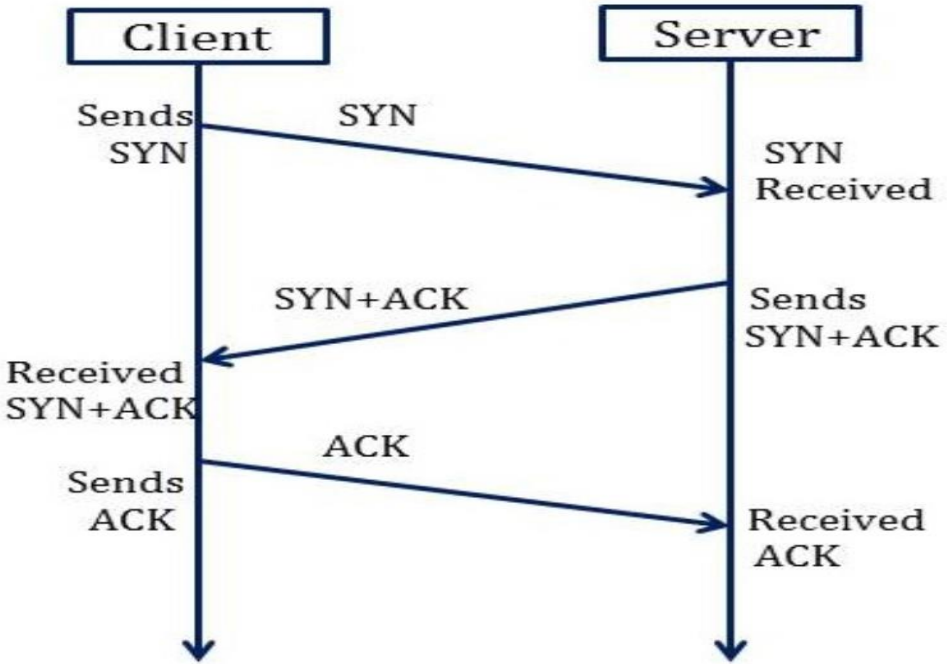
A socket is a combination of port and IP address. (IP ADDRESS + PORT)

There are 65,535 possible port numbers, although not all are in common use. Some of the most commonly used ports, along with their associated networking protocol, are

0 - 1023 are well known ports

Service, Protocol, or Application	Port Number	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System	53	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
IMAP4	143	TCP

TCP Three-way Handshake



Explanation of Three-way handshake Mechanism

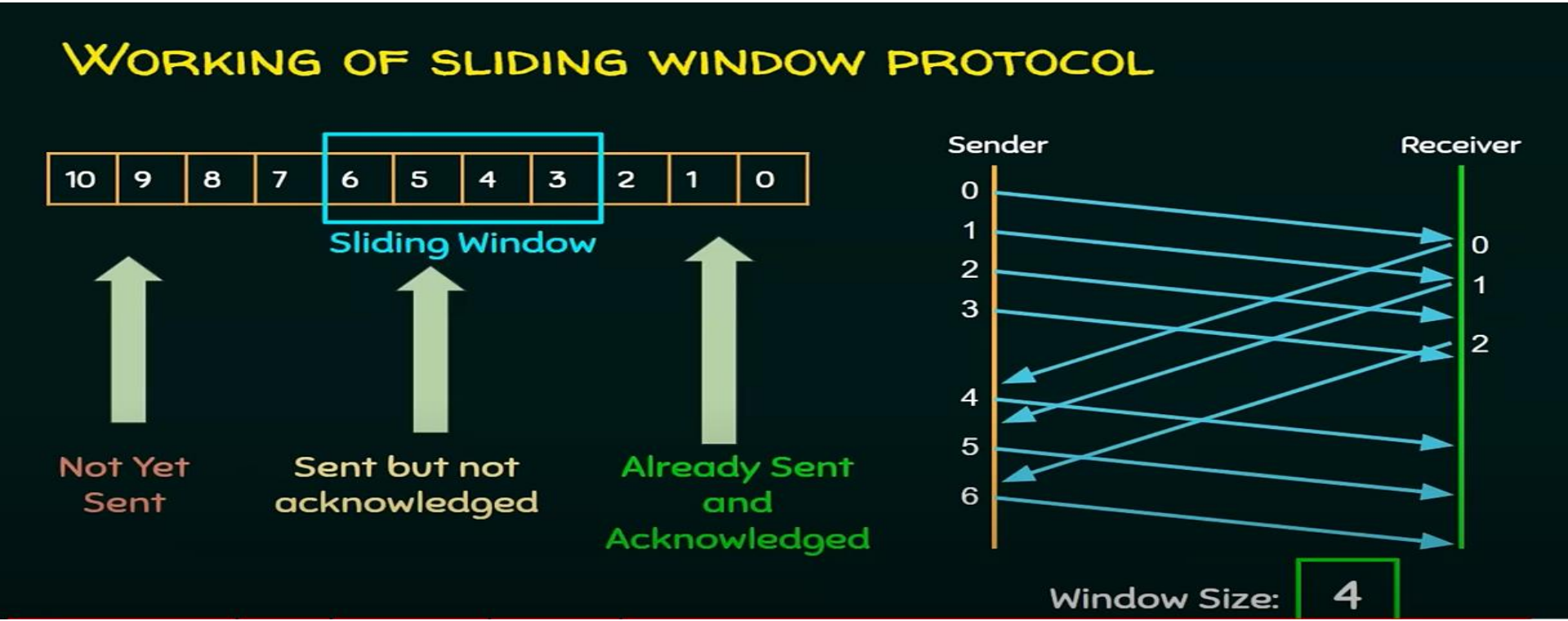
1. Connection Initiation:
    - Client sends a SYN (synchronize) packet to the server, indicating its intent to establish a connection.
    - The SYN packet contains a sequence number chosen by the client to start the connection.
2. Acknowledgment and Agreement:
    - Upon receiving the SYN packet, the server responds with a SYN-ACK (synchronize-acknowledgment) packet.
    - The SYN-ACK packet acknowledges the client's SYN packet and contains the server's own chosen sequence number.
3. Finalizing the Connection:
    - Finally, the client acknowledges the server's SYN-ACK packet by sending an ACK packet.
    - This ACK packet confirms the server's acknowledgment and completes the three-way handshake.

Flow Control In Transport Layer

Flow control mechanisms in the transport layer regulate the rate of data transmission between sender and receiver to ensure that the sender does not overwhelm the receiver.

1. Sliding Window Protocol:
    - TCP uses a sliding window protocol for flow control. This window represents the amount of data that the sender can transmit before receiving an acknowledgment from the receiver.
    - Send Multiple Frames at a time.
    - Number of frames to be sent is based on window size.
    - Each frame is numbered which we call as sequence number.

Working of Sliding Window



Congestion Control

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.

Comparison of Leaky Bucket and Token Bucket

- Both algorithms are used for traffic shaping and policing, but they have different approaches to controlling the rate of data transmission.
- The leaky bucket algorithm maintains a constant output rate, while the token bucket algorithm allows for bursts of traffic as long as tokens are available.
- The token bucket algorithm offers more flexibility in regulating traffic and supporting different QoS levels compared to the leaky bucket algorithm.