NETWORK & SECURITY

CHEATSHEET

ACCENTURE

PRIME CODING

OSI Model Layers

- Layer 1: Physical Layer
  - Function: Transmission of raw bit streams over a physical medium.
  - Examples:
    - Ethernet Cables: These cables are used to physically connect devices in a network, transmitting data in the form of electrical signals.
    - Hubs: A hub is a basic networking device that connects multiple devices in a network, forwarding data to all connected devices. It operates purely on the physical layer, transmitting the signal to all devices without any filtering or routing.

OSI Model Layers

- Layer 2: Data Link Layer
- Function: Node-to-node data transfer and error detection.
    - MAC Addresses: A Media Access Control (MAC) address is a unique identifier assigned to network interfaces for communications at the data link layer. It helps in identifying the devices on the local network.
        - Example: 00:1A:2B:3C:4D:5E
    - Switches: A switch is a device that connects devices within the same network. Unlike hubs, switches operate at the data link layer and can use MAC addresses to forward data to the correct device on the network.

OSI Model Layers

- Layer 3: Network Layer
- Function: Logical addressing and routing.
- Examples:
  - IP Addresses: An IP address is a logical address assigned to devices connected to a network, enabling them to be identified and located. This layer manages the routing of packets based on IP addresses.
    - IPv4 Example: 192.168.1.1
  - Routers: Routers are devices that forward data packets between different networks, based on the destination IP address. They operate at the network layer and determine the best path for data to travel from the source to the destination.

- Layer 4: Transport Layer
- Function: End-to-end communication, reliability, and flow control.
- Examples:
  - TCP (Transmission Control Protocol): TCP is a connection-oriented protocol that ensures reliable data transmission between devices. It establishes a connection, ensures data is received, and retransmits any lost packets.
  - UDP (User Datagram Protocol): UDP is a connectionless protocol that allows data to be sent without establishing a connection. It is faster but less reliable than TCP, often used for streaming media where speed is more critical than accuracy.

- Layer 5: Session Layer
- Function: Establishment, management, and termination of sessions.
- Examples:
  - APIs (Application Programming Interfaces): APIs facilitate communication between different software applications, establishing a session to exchange data.
  - Sockets: A socket is an endpoint for sending and receiving data across a network, allowing communication between a client and a server.

- Layer 6: Presentation Layer
- Function: Data translation, encryption, and compression.
- Examples:
  - SSL (Secure Sockets Layer): SSL is a protocol used to encrypt data between a web server and a browser, ensuring secure communication. It operates at the presentation layer to encrypt and decrypt data.
  - JPEG (Joint Photographic Experts Group): JPEG is a commonly used method of compressing digital images, reducing file size while maintaining quality.
  - MPEG (Moving Picture Experts Group): MPEG is a standard for compressing video and audio data, allowing for efficient storage and transmission of multimedia content.

- Layer 7: Application Layer
- Function: End-user services and application interfaces.
- Examples:
  - HTTP (HyperText Transfer Protocol): HTTP is the protocol used for transmitting web pages on the internet. It enables communication between a web browser and a web server.
  - FTP (File Transfer Protocol): FTP is a protocol used to transfer files between computers on a network. It allows users to upload and download files from a server.
  - SMTP (Simple Mail Transfer Protocol): SMTP is a protocol used for sending and receiving email messages across networks.

Common Network Devices

- Router
  - Function: Routes data between different networks using IP addresses.
  - Scenario: Used when connecting multiple networks (e.g., LAN to WAN).
- Switch
  - Function: Connects devices within the same network and uses MAC addresses to forward data.
  - Scenario: Ideal for expanding the number of devices in a local network.

Common Network Devices

- Firewall
  - Function: Monitors and controls incoming and outgoing network traffic based on predetermined security rules.
  - Scenario: Protects networks by filtering traffic and blocking unauthorized access.
- Access Point
  - Function: Allows wireless devices to connect to a wired network using Wi-Fi.
  - Scenario: Used in wireless LANs (WLANs) to extend the network's reach.

IP Addressing & Subnetting

- IPv4 Addressing
  - Format: 32-bit number, written in dotted decimal (e.g., 192.168.1.1).
  - Classes:
  - Class A:
    - Range: 0.0.0.0 to 127.255.255.255
    - Usage: Designed for very large networks, with the first octet (8 bits) representing the network portion and the remaining 24 bits representing the host portion. It supports up to 16 million hosts on each of 128 networks

IP Addressing & Subnetting

- Class B:
  - Range: 128.0.0.0 to 191.255.255.255
  - Usage: Used for medium-sized networks, with the first two octets representing the network portion and the remaining 16 bits for hosts. It supports up to 65,000 hosts on each of 16,000 networks.
- Class C:
  - Range: 192.0.0.0 to 223.255.255.255
  - Usage: Suited for smaller networks, with the first three octets representing the network portion and the last octet for hosts. It supports 254 hosts on each of 2 million networks.

IP Addressing & Subnetting

- IPv6 Addressing
- Format: IPv6 addresses are 128-bit numbers, written in hexadecimal format and separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). The addresses are divided into eight 16-bit blocks.

IP Addressing & Subnetting

Key Features:

- Extended Address Space: Unlike IPv4, which supports approximately 4.3 billion unique addresses, IPv6 supports an astronomical number of addresses, approximately 3.4×10^38, due to its 128-bit length.
- Simplified Addressing: IPv6 reduces the need for Network Address Translation (NAT) by providing a vastly larger address space.
- Representation: Consecutive sections of zeros can be abbreviated with :: (e.g., 2001:0db8:0000:0000:0000:0000:1428:57ab can be shortened to 2001:db8::1428:57ab).

IP Addressing & Subnetting

Types of IPv6 Addresses:

- Unicast: A single address identifying a unique interface on a device. Used for one-to-one communication.
- Anycast: Addresses that identify multiple interfaces but are delivered to the nearest one (in terms of routing distance).
- Multicast: Addresses used to send data to multiple interfaces simultaneously (one-to-many communication).

IP Addressing & Subnetting

Key Differences Between IPv4 and IPv6:

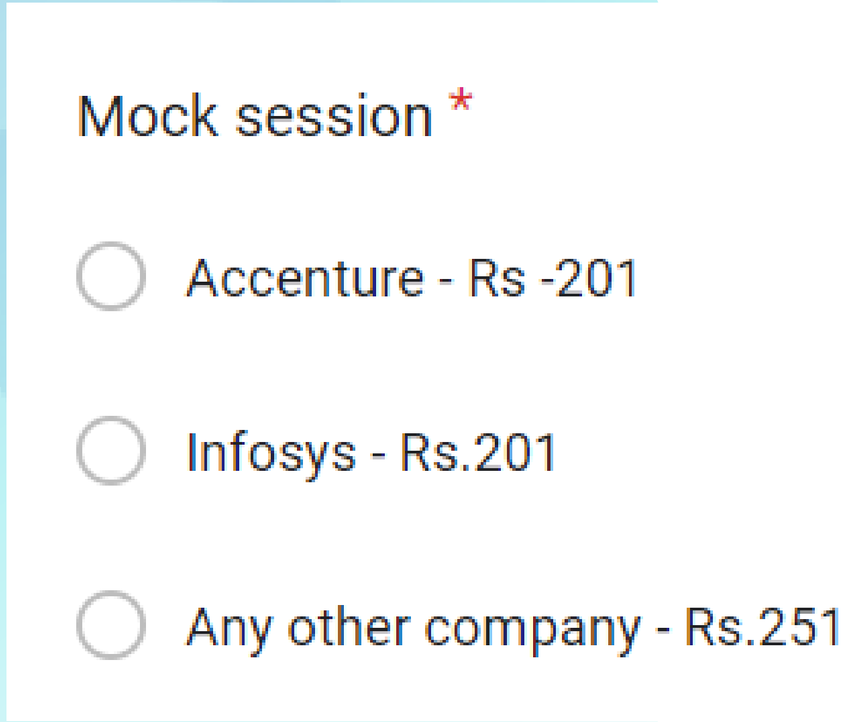
- Address Size: IPv4 is 32-bit, IPv6 is 128-bit.
- Addressing Format: IPv4 uses decimal, IPv6 uses hexadecimal.
- Address Space: IPv6 has a vastly larger address space compared to IPv4.
- Header Complexity: IPv6 simplifies the header structure, improving processing efficiency.

IP Addressing & Subnetting

- Subnetting
  - Purpose: Divides a network into smaller subnets for better management and security.
  - Example: Subnetting a Class C network (e.g., 192.168.1.0/24) into smaller subnets using different subnet masks like /25, /26, etc.

1:1 MOCK SESSION

Special: Exclusive 48-Hour Discount for Female Candidates!



Link in Description

Success Stories: Candidates Thank Us for Their Interview Triumph

Adesh Kulkarni SUCCESS STORY

THROUGH **TELEGRAM**

Sir I want to share good news! I got into TCS.
The mock sessions by you and Aditya sir were so helpful. Many questions were similar. Also your videos were spot-on for cracking TCS. Thank you for all the support.

Moulik SUCCESS STORY

THROUGH **TELEGRAM**

Bhaiya my tcs digital is cleared, Thanks a lot. Your mock session was very beneficial. Couldn't have done it without it.

Vikram Reddy SUCCESS STORY

THROUGH **TELEGRAM**

I got a digital offer today
Thanks. Your mock interview helped me a lot in cracking the interview .It helped me in boosting my confidence It was really helpful for me 💗
Thanks a lot

Access Control Lists (ACLs)

- Standard ACL
  - Function: Filters traffic based solely on source IP addresses.
  - Example: access-list 10 deny 192.168.1.0 0.0.0.255
- Extended ACL
  - Function: Filters traffic based on both source and destination IP addresses, ports, and protocols.
  - Example: access-list 110 permit tcp any host 192.168.1.10 eq 80

Network Security Concepts

- Encryption
  - Function: Transforms data into an unreadable format to prevent unauthorized access.
  - Example: SSL/TLS for secure web communication.
- Firewalls
  - Types: Hardware, software, or both.
  - Example: Configuring a firewall to block all incoming traffic except on port 443 (HTTPS).

Network Security Concepts

- Intrusion Detection System (IDS)
  - Function: Monitors network traffic for suspicious activity and known threats.
  - Example: Snort, a popular open-source IDS.
- Virtual Private Network (VPN)
  - Function: Creates a secure, encrypted connection over a less secure network, such as the internet.
  - Example: Remote workers accessing company resources via VPN.

Security Protocols

- **HTTPS (Hypertext Transfer Protocol Secure)**
  - Use: Secure communication over the internet by encrypting data between the browser and server.
- **IPsec (Internet Protocol Security)**
  - Use: Secures IP communication by authenticating and encrypting each IP packet.
- **SSH (Secure Shell)**
  - Use: Secure remote access to network devices and servers.
- **TLS (Transport Layer Security)**
  - Use: Successor to SSL, provides end-to-end security of data sent between applications over the internet.

Types of Cyber Attacks

- **Phishing**
  - Function: Fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.
  - Example: Fake emails or websites mimicking legitimate services to steal login credentials.
- **DDoS (Distributed Denial of Service)**
  - Function: Overwhelms a network or service with excessive traffic to render it unusable.
  - Example: Attacking a website with a botnet to make it inaccessible.
- **Ransomware**
  - Function: Encrypts the victim's data and demands payment for the decryption key.
  - Example: WannaCry ransomware attack.

Questions on Cyber Attacks

- **Which type of cyberattack involves overwhelming a network or service with excessive traffic, making it inaccessible to users?**
  - **Answer: DDoS (Distributed Denial of Service)**

- **Which cybersecurity threat encrypts a victim's data and demands payment for the decryption key?**
  - **Answer: Ransomware**

- **Which form of cyberattack involves tricking individuals into providing sensitive information by pretending to be a trustworthy entity?**
  - **Answer: Phishing**

Network Troubleshooting Commands

- **ping**
  - Use: Checks the connectivity between two devices.
  - Example: ping 192.168.1.1
- **traceroute (tracert on Windows)**
  - Use: Traces the path packets take to reach a destination.
  - Example: tracert google.com
- **nslookup**
  - Use: Queries DNS to obtain domain name or IP address mapping.
  - Example: nslookup www.example.com
- **netstat**
  - Use: Displays network connections, routing tables , and interface statistics.
  - Example: netstat -an

THANK YOU