**NETWORKING**

1. TCP/IP:-

TCP/IP is the backbone of the internet and forms the basis of all network communication. Understanding how TCP/IP works is essential for troubleshooting network issues and optimizing application performance. TCP (Transmission Control Protocol) breaks data into packets, sends them across the network, and ensures they are reassembled correctly on the receiving end. IP (Internet Protocol) is responsible for routing the packets to their intended destination.

2. DNS:-

DNS (Domain Name System) translates human-readable domain names into IP addresses, enabling users to access websites and services without needing to remember a string of numbers. As a DevOps engineer, you’ll need to understand how DNS works, how to configure DNS servers, and how to troubleshoot DNS issues.

3. Load Balancing:-

Load Balancing distributes incoming network traffic across multiple servers, ensuring that no single server becomes overloaded. This helps to improve application performance, scalability, and availability. DevOps engineers need to know how to configure load balancers and monitor their performance to ensure that they are functioning correctly.

4. Security:-

Network security is a critical concern for DevOps engineers, and understanding how to secure networks and applications is essential. Concepts such as firewalls, VPNs (Virtual Private Networks), and SSL (Secure Sockets Layer) encryption are essential components of a secure network. DevOps engineers need to be familiar with security best practices and implement them at every stage of the application lifecycle.

5. IP Addressing and Subnetting:-

IP addressing is a method of assigning unique numerical identifiers to devices connected to a network. It allows devices to communicate with each other using the Internet Protocol (IP). Subnetting involves dividing a large network into smaller subnetworks, known as subnets. It helps in efficient allocation of IP addresses and facilitates network segmentation, which enhances security and improves network performance

6. DHCP:-

DHCP is a protocol that automates the assignment of IP addresses to devices on a network. DHCP eliminates the manual configuration of IP addresses, making it easier to manage and scale network deployments. Understanding DNS and DHCP is essential for configuring and maintaining network infrastructure effectively.

7. Routing and Switching:-

Routing involves the process of determining the path that network packets should take from source to destination. It utilizes routing protocols, such as OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol), to make routing decisions. Switching, on the other hand, involves forwarding data packets between devices within a network.

Routing ensures efficient and secure data transmission across networks. It optimizes traffic flow, improves network performance, and enables connectivity between different network segments. Switching facilitates communication within a network by forwarding packets to the correct destinations. Knowledge of routing and switching is vital for designing scalable and robust network architectures.

8. Types of Network Protocols:

i. Network Communication protocols

ii. Network Security Protocols

iii. Network Management Protocols

**Network Communication Protocol** — It describes establishing and maintaining connection and communication. As you work with different devices and network services, you’ll make use of various network communication protocols.

Transmission Control Protocol: TCP chunks up data into data packets that can be sent securely and quickly while minimizing the chance of data loss.

Internet Protocol: IP is responsible for the addressing of a data packet. IP encapsulates the data packet to be delivered and adds an address header. The header contains information on the sender and recipient IP addresses.

User Datagram Protocol: UDP is a connection-less protocol that offers a low-latency and loss-tolerant implementation.

Hypertext Transfer Protocol (HTTP): The HTTP protocol uses TCP/IP to deliver web page content from a server to your browser. HTTP can also handle the download and upload of files from remote servers.

File Transfer Protocol (FTP): FTP is used to transfer files between different computers on a network. Typically, you’d use FTP to upload files to a server from a remote location.

Post Office Protocol 3 (POP3): POP3 is one of three email protocols. It’s most commonly used by an email client to allow you to receive emails. This protocol uses TCP for the management and delivery of an email.

Simple Mail Transfer Protocol (SMTP): SMTP is another one of the three email protocols. It’s most commonly used to send emails from an email client via an email server. This protocol uses the TCP for the management and transmission of the email.

Interactive Mail Access Protocol (IMAP): IMAP is the more powerful of the three email protocols. With IMAP and an email client, you can manage a single mailbox on an email server in your organization.

**Networking Security Protocol** — Network security protocols are designed to maintain the security and network of data across your network. To implement a secure network, you must match the right security protocols.

Secure Socket Layer (SSL): SSL is a standard encryption and security protocol. It provides a secure and encrypted connection between your computer and the target server or device that you accessed over the internet.

Transport Layer Security (TLS): TLS is the successor to SSL, and provides a stronger and more robust security encryption protocol.

Hypertext Transfer Protocol Secure (HTTPS): HTTPS provides a more secure version of the standard HTTP protocol by using the TLS or SSL encryption standard.

Secure Shell (SSH): SSH is a cryptographic network security protocol that provides a secure data connection across a network.

Kerberos: This validation protocol provides a robust authentication for client-server-based applications through secret-key cryptography. Kerberos assumes that all endpoints in the network are insecure. It enforces strong encryption for all communications and data at all times.

**Network management protocols** — The focus of this type of protocol is the sustainability of the network by looking at faults and performance. Two network management protocols are available:

Simple Network Management Protocol (SNMP): SNMP is an internet protocol that allows for the collection of data from devices on your network and the management of those devices.

Internet Control Message Protocol (ICMP): ICMP is one of the protocols included within the Internet Protocol suite (IPS). It allows network-connected devices to send warning and error messages, along with operation information about the success or failure of a connection request, or if a service is unavailable.