Module 3 [Network Configuration]

By:- Purv Patel

Topic: Local area networking

1. What is network?

A network, in the context of technology, typically refers to a collection of interconnected devices or nodes that can communicate with each other. These devices can include computers, servers, routers, switches, printers, and other hardware. The purpose of a network is to enable communication and the sharing of resources, such as files, applications, and internet connections, among the connected devices.

1. What is intranet and internet?

Intranet and internet are two types of networks, each serving different purposes:

1. Intranet:

- An intranet is a private network that is confined within an organization or a specific group of users.

- It is used to facilitate internal communication, collaboration, and information sharing among employees or members of the organization.

- Intranets typically use technologies such as LANs (Local Area Networks) or WANs (Wide Area Networks) to connect computers and other devices within the organization.

- Access to an intranet is usually restricted to authorized users, often requiring login credentials or other authentication mechanisms.

- Intranets commonly host internal websites, databases, document repositories, and other resources that are accessible only to individuals within the organization.

2. Internet:

- The internet is a global network that connects millions of computers, devices, and networks worldwide.

- It is a public network that allows users to access information, services, and resources from virtually anywhere in the world.

- The internet is based on a decentralized architecture, with interconnected networks using standardized communication protocols such as TCP/IP (Transmission Control Protocol/Internet Protocol).

- Users access the internet through Internet Service Providers (ISPs) using various technologies such as dial-up, DSL, cable, Fiber-optic, or mobile networks.

- The internet enables a wide range of activities, including browsing websites, sending and receiving emails, accessing cloud services, streaming media, online gaming, and much more.

- Unlike intranets, which are private and restricted to specific users or organizations, the internet is open to anyone with an internet connection.

In summary, while an intranet is a private network used for internal communication and collaboration within an organization, the internet is a global network that connects users and resources worldwide, enabling communication, information sharing, and access to online services on a massive scale.

1. How many types of networks we use?

There are several types of networks that we commonly use, each serving different purposes and operating at various scales. Here are some of the main types:

1. Local Area Network (LAN)

2. Wide Area Network

3. Metropolitan Area Network (MAN)

4. Personal Area Network (PAN):

5. Home Area Network (HAN

6. Wireless Local Area Network (WLAN)

7. Cellular Network

8. Satellite Network

9. Sensor Network

10. Virtual Private Network (VPN)

1. Differentiate between LAN and PAN.

Local Area Network (LAN):

Definition: A LAN is a network that typically spans a small geographical area, such as a single building, office, or campus.

Scope: LANs are used to connect devices within a limited area to facilitate communication, resource sharing, and data exchange.

Technologies: LANs often utilize wired technologies like Ethernet or wireless technologies like Wi-Fi to interconnect devices such as computers, printers, servers, and other networked devices.

Usage: LANs are commonly deployed in homes, businesses, schools, and other organizations to enable local communication and access to shared resources.

Personal Area Network (PAN):

Definition: A PAN is a network formed by interconnecting personal devices over a short distance, typically within a person's immediate surroundings.

Scope: PANs are designed for personal use and typically cover a very small area, such as a room or a person's body.

Technologies: PANs often use wireless technologies such as Bluetooth, Zigbee, or Near Field Communication (NFC) to connect devices like smartphones, tablets, laptops, wearable devices, and peripherals.

Usage: PANs facilitate communication and data exchange between personal devices, such as syncing a smartphone with a smartwatch, connecting a wireless keyboard and mouse to a computer, or transferring files between devices.

1. Explain LAN

LAN stands for Local Area Network. It is a network that covers a small geographic area, such as a single building, office, or campus. LANs connect computers, servers, printers, and other devices within the same physical location. They facilitate local communication, resource sharing, and collaboration among users. LANs can use both wired (Ethernet) and wireless (Wi-Fi) technologies. They are commonly used in offices, schools, homes, and small businesses to provide internet access, file sharing, and other network services.

1. What are the different types of LAN devices?
2. Computers/Workstations: Used by users to access network resources.
3. Servers: Store and manage data, provide services to clients.
4. Routers: Connect LANs, forward data between networks.
5. Switches: Connect devices within a LAN, forward data to intended recipients.
6. Access Points: Create wireless LANs, enable wireless device connectivity.
7. Network Interface Cards (NICs): Enable devices to connect to the network.
8. Printers: Shared among users for printing documents.
9. Network Attached Storage (NAS): Centralized storage and file sharing.
10. Firewalls: Control and monitor network traffic, enhance security.

Modems: Connect LANs to the internet or other networks.

1. Network Hubs: Less common, broadcast data to all devices in a LAN.

Top of Form

## Topic: configured network

1. What is configured network?

Configuring a network involves setting up devices and settings to enable communication and resource sharing. Here's a concise overview of the steps involved:

Plan Network Layout: Determine the network's scope, including the number and types of devices, their locations, and how they'll be connected (wired or wireless).

Assign IP Addresses: Assign unique IP addresses to each device on the network to enable communication. This can be done manually or using Dynamic Host Configuration Protocol (DHCP) for automatic assignment.

Configure Network Devices: Set up routers, switches, access points, and other network devices with appropriate settings, including IP addresses, subnet masks, gateway addresses, and DNS servers.

Secure the Network: Implement security measures such as setting strong passwords, enabling encryption (e.g., WPA2 for Wi-Fi), configuring firewalls, and restricting access to sensitive resources.

Test Connectivity: Verify that devices can communicate with each other and access network resources. Troubleshoot any connectivity issues and adjust configurations as needed.

Document Network Configuration: Keep records of network settings, device configurations, and any changes made for future reference and troubleshooting.

1. How do we configure network?

Configuring a network involves several steps. Here's a general guide on how to configure a network:

1. Plan the Network:

- Determine the layout of your network, including the number of devices, their locations, and how they will be connected (wired or wireless).

2. \*\*Assign IP Addresses:

- Assign unique IP addresses to each device on the network. You can do this manually by setting static IP addresses or use Dynamic Host Configuration Protocol (DHCP) for automatic assignment.

3. \*\*Set Up Network Devices: \*\*

- Configure routers, switches, access points, and other network devices with appropriate settings.

- Set IP addresses, subnet masks, gateway addresses, and DNS servers on each device.

- Configure wireless settings if setting up a wireless network, including SSID, encryption method, and passphrase.

4. \*\*Secure the Network: \*\*

- Implement security measures to protect your network from unauthorized access and attacks.

- Set strong passwords for network devices and Wi-Fi networks.

- Enable encryption (e.g., WPA2) for wireless networks.

- Configure firewalls to control traffic and block malicious activities.

- Restrict access to sensitive resources using access control lists (ACLs) or VLANs.

5. \*\*Test Connectivity: \*\*

- Verify that devices can communicate with each other and access network resources.

- Use ping, traceroute, or other network diagnostic tools to test connectivity and troubleshoot any issues.

6. \*\*Document Network Configuration: \*\*

- Keep records of network settings, device configurations, and any changes made for future reference and troubleshooting.

- Document the network topology, IP addressing scheme, and security policies.

7. \*\*Monitor and Maintain the Network: \*\*

- Regularly monitor network performance and security.

- Update firmware and software on network devices to ensure they are up-to-date and secure.

- Make adjustments to network configurations as needed to optimize performance and address changing requirements.

1. How to check IP address?

Open the Command Prompt by typing "cmd" in the Windows search bar and pressing Enter.

In the Command Prompt window, type the command "ipconfig" and press Enter.

Look for the "IPv4 Address" under the network adapter you're using. This address is your IP address

1. How to check the IP address by cmd?

Open the Command Prompt by typing "cmd" in the Windows search bar and pressing Enter.

In the Command Prompt window, type the command "ipconfig" and press Enter.

Look for the "IPv4 Address" under the network adapter you're using. This address is your IP address.

1. How can we enter static address in network adapter?

To enter a static IP address for a network adapter, follow these general steps:

1. \*\*Open Network Settings: \*\*

- On Windows: Go to Settings > Network & Internet > Change adapter options.

- On macOS: Go to System Preferences > Network.

- On Linux: The process varies depending on the distribution, but typically involves accessing network settings through the system settings or network manager applet.

2. \*\*Select Network Adapter: \*\*

- Choose the network adapter for which you want to set a static IP address. This could be Ethernet, Wi-Fi, or any other network interface.

3. \*\*Access Adapter Properties: \*\*

- On Windows: Right-click on the network adapter and select Properties.

- On macOS: Click on the network adapter, then click on the gear icon (⚙️) and select Configure IPv4 (or IPv6) > Manually.

- On Linux: Right-click on the network adapter and select Edit Connections or similar option.

4. \*\*Configure IP Address Settings: \*\*

- Look for the option to manually set the IP address, subnet mask, default gateway, and DNS server addresses.

- Enter the desired IP address, subnet mask, gateway, and DNS server addresses in the corresponding fields.

5. \*\*Save Settings: \*\*

- After entering the static IP address and related settings, save the changes by clicking Apply or OK.

6. \*\*Verify Configuration: \*\*

- After saving the settings, verify that the network adapter is now using the static IP address by checking the adapter properties again or using the appropriate command-line tool (e.g., "ipconfig" on Windows, "ipconfig" on macOS and Linux)

## Topic: wireless networking

1. What is the difference between WEP and WPA?

- \*\*WEP (Wired Equivalent Privacy) \*\*: Older, weaker security protocol for wireless networks. Uses static encryption keys, vulnerable to easy cracking, lacks robust authentication and key management.

- \*\*WPA (Wi-Fi Protected Access) \*\*: Improved security protocol addressing WEP's weaknesses. Introduces dynamic encryption keys, stronger authentication methods, and better key management. Provides better security and compatibility compared to WEP.

1. What is wireless network?

- \*\*Wireless Network\*\*: A network that enables communication between devices without the need for physical cables. Utilizes wireless technologies such as Wi-Fi, Bluetooth, or infrared to transmit data over the airwaves.

- \*\*Components\*\*: Includes devices like routers, access points, and wireless adapters. Routers create wireless networks, access points extend coverage, and wireless adapters enable devices to connect wirelessly.

- \*\*Security\*\*: Important to secure wireless networks to prevent unauthorized access. Common security measures include encryption (WPA2/WPA3), strong passwords, and disabling SSID broadcasting.

- \*\*Advantages\*\*: Provides flexibility, mobility, and convenience, allowing devices to connect to the internet or share data without being tethered to a physical connection.

- \*\*Applications\*\*: Widely used in homes, businesses, schools, and public spaces for internet access, file sharing, communication, and IoT devices.

1. What is wireless network connection?

Wireless Network Connection: The process of establishing a connection between a device and a wireless network, typically using Wi-Fi technology.

1. What are the basic concepts of networking?

Basic concepts of networking include:

1. \*\*Network\*\*: A collection of devices connected together to share resources and communicate.

2. \*\*Node\*\*: Any device connected to a network, such as computers, servers, routers, switches, printers, etc.

3. \*\*Protocol\*\*: A set of rules and conventions that govern how data is transmitted and received over a network.

4. \*\*IP Address\*\*: A unique identifier assigned to each device on a network for communication purposes.

5. \*\*MAC Address\*\*: A hardware address assigned to each network interface card (NIC) for identification on a network.

6. \*\*Router\*\*: A networking device that forwards data packets between computer networks. It connects multiple networks together.

7. \*\*Switch\*\*: A networking device that connects devices within the same network and forwards data packets to the intended recipient.

8. \*\*Gateway\*\*: A device that serves as an entry and exit point between two different networks, typically connecting a LAN to the internet.

9. \*\*LAN (Local Area Network) \*\*: A network that covers a small geographic area, such as a single building or office.

10. \*\*WAN (Wide Area Network) \*\*: A network that covers a large geographic area, such as multiple buildings, cities, or countries.

11. \*\*Topology\*\*: The physical or logical layout of devices and connections in a network, such as bus, star, ring, mesh, or hybrid.

12. \*\*Protocol Stack\*\*: A set of networking protocols organized in layers, such as TCP/IP (Transmission Control Protocol/Internet Protocol) or OSI (Open Systems Interconnection) model.

13. \*\*DNS (Domain Name System) \*\*: A system that translates domain names into IP addresses, allowing users to access websites using human-readable names.

14. \*\*DHCP (Dynamic Host Configuration Protocol) \*\*: A network protocol used to automatically assign IP addresses and other network configuration parameters to devices.

15. \*\*Firewall\*\*: A security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

1. What do you need to know about networking?

1. \*\*Network Types and Topologies\*\*: Understand the different types of networks such as LANs, WANs, MANs, PANs, and their respective topologies (e.g., bus, star, ring).

2. \*\*Network Devices and Components\*\*: Learn about devices like routers, switches, hubs, access points, NICs, and their roles in network communication.

3. \*\*Networking Protocols\*\*: Gain knowledge of protocols such as TCP/IP, OSI model, Ethernet, Wi-Fi (802.11), DNS, DHCP, HTTP, HTTPS, FTP, SNMP, and others.

4. \*\*IP Addressing and Subnetting\*\*: Understand IPv4 and IPv6 addressing, subnet masks, CIDR notation, DHCP, static vs. dynamic IP addressing, and subnetting principles.

5. \*\*Routing and Switching\*\*: Learn about routing protocols (e.g., RIP, OSPF, BGP) for forwarding packets between networks, and switching technologies for forwarding packets within a network.

6. \*\*Wireless Networking\*\*: Familiarize yourself with Wi-Fi standards, security protocols (WEP, WPA, WPA2, WPA3), SSIDs, channels, and interference mitigation techniques.

7. \*\*Network Security\*\*: Understand common security threats (e.g., malware, phishing, DDoS attacks), encryption techniques (e.g., SSL/TLS, AES), firewalls, VPNs, and intrusion detection/prevention systems (IDS/IPS).

8. \*\*Network Management and Monitoring\*\*: Learn about network management tools (e.g., SNMP, Syslog, NetFlow), monitoring techniques, performance optimization, and troubleshooting methodologies.

9. \*\*Cloud Computing and Virtualization\*\*: Understand how networks are configured, managed, and secured in cloud environments, and the concepts of virtualization (e.g., virtual LANs, virtual machines).

10. \*\*Emerging Technologies\*\*: Stay updated on emerging networking technologies such as SDN (Software-Defined Networking), NFV (Network Functions Virtualization), IoT (Internet of Things), 5G, and edge computing.

1. \*\*Certifications\*\*: Consider pursuing industry-standard certifications such as CompTIA Network+, Cisco CCNA, CCNP, CCIE, or others to validate your networking knowledge and skills
2. What do u know about computer networking?

Computer networking involves connecting multiple devices to share resources and information.

Types of networks include LANs (Local Area Networks), WANs (Wide Area Networks), MANs (Metropolitan Area Networks), and PANs (Personal Area Networks).

Network components include devices (computers, servers, routers), media (wired and wireless transmission), and protocols (TCP/IP, Ethernet, Wi-Fi).

Key aspects of networking include network architecture, protocols, security, services, and management.

Networking facilitates communication, collaboration, and resource sharing across devices and environments.

## Topic: the internet

1. What do u mean by the term URL?

"URL" stands for Uniform Resource Locator, and it is a web address used to locate a specific resource on the internet. When you refer to "URL in short," you might be asking for a shortened URL, which is a condensed version of a longer URL that directs users to the same web page. Services like Bitly or Tiny URL are commonly used to create shortened URLs.

1. Term which is use to see web pages is called?

The term commonly used to refer to viewing web pages is "browsing" or "web browsing." When someone accesses a website or navigates through different pages on the internet, they are said to be browsing the web.

1. In the Ethernet which topology is used?

In Ethernet networks, the most commonly used topology is the "star" topology. In a star topology, each network device (such as computers, printers, etc.) is connected directly to a central hub or switch. This central hub or switch manages the network traffic by routing data between the connected devices. The star topology offers advantages such as easy scalability, simplified troubleshooting, and the ability to isolate network issues to specific segments.

1. Set of rules and regulations while working on internet, which term is used?

a protocol refers to a set of rules or conventions that govern how data is transmitted and received between devices or systems. Various protocols, such as TCP/IP, HTTP, DNS, SMTP, POP, IMAP, and FTP, facilitate different types of communication and tasks on the internet.

1. What do u mean by RAS?

RAS stands for Remote Access Service. It is a technology that enables users to connect remotely to a network or computer system over a telecommunications network. RAS allows users to access resources such as files, printers, and applications as if they were directly connected to the network or computer system. This technology is commonly used for telecommuting, remote administration, and providing remote support to users.

1. What are the main search engines to get more website URL on internet?

Google

Bing

Yahoo

DuckDuckGo

Baidu

Yandex

1. What does the protocol consist of?

A protocol consists of a set of rules or conventions that define how data is transmitted and received between devices or systems in a network. These rules govern various aspects of communication, including the format of data packets, the order of data transmission, error detection and correction mechanisms, addressing schemes, and procedures for establishing and terminating connections.

In the context of networking, protocols ensure interoperability between different devices and systems by providing a standardized way for them to communicate with each other. Each protocol specifies how information is exchanged, interpreted, and processed, allowing devices from different manufacturers and running different software to communicate effectively.

Protocols can operate at different layers of the networking stack, such as the physical layer (e.g., Ethernet), data link layer (e.g., Wi-Fi), network layer (e.g., IP), transport layer (e.g., TCP), and application layer (e.g., HTTP). Each layer may have its own set of protocols responsible for specific functions related to data transmission and network communication.

## Topc: virtualization

1. What is virtualization?

Virtualization is a technology that creates virtual versions of hardware, operating systems, storage, or networks. It allows multiple virtual instances to run on a single physical machine, improving resource utilization, flexibility, and management.

1. What is the difference between full virtualization and para virtualization?

The difference between full virtualization and para-virtualization lies in how they handle virtualization of hardware resources:

1. \*\*Full Virtualization\*\*: In full virtualization, the virtualization layer (called a hypervisor) presents a complete virtual replica of the underlying physical hardware to the guest operating systems. The guest operating systems are unaware that they are running in a virtualized environment and operate as if they are running on dedicated physical hardware. This approach typically requires no modifications to the guest operating systems, making it easier to migrate existing systems to a virtualized environment.

1. \*\*Para-virtualization\*\*: In para-virtualization, the guest operating systems are modified to be aware of the virtualization layer. Instead of presenting a complete virtual replica of the hardware, the hypervisor provides a set of modified interfaces that the guest operating systems can use to communicate with the underlying physical hardware. This allows for more efficient communication between the guest operating systems and the hypervisor, leading to better performance compared to full virtualization in certain scenarios. However, para-virtualization requires modifications to the guest operating systems, which may not be feasible for all environments

3.what is hyper visor?

In short, a hypervisor is a software layer that enables virtualization by creating and managing virtual machines on physical hardware. It allows multiple operating systems or virtual machines to share the same physical resources. There are two main types: Type 1 runs directly on hardware, while Type 2 runs on top of an operating system.

1. What is difference between hypervisor available in Linux?

In short, Linux offers two main types of hypervisors: Type 1, which includes Xen and KVM, runs directly on hardware; Type 2, such as VirtualBox and QEMU, runs on top of a host operating system. Type 1 is suited for server virtualization, while Type 2 is often used for desktop or testing purposes.

1. What is Virtualization and its types?

In short, virtualization is the technology of creating virtual versions of hardware, software, storage, or networks. Its main types are:

1. \*\*Server Virtualization\*\*: Divides a physical server into multiple virtual servers.

2. \*\*Desktop Virtualization\*\*: Enables multiple virtual desktop instances on a single physical machine.

3. \*\*Storage Virtualization\*\*: Abstracts physical storage into a virtual pool of resources.

4. \*\*Network Virtualization\*\*: Creates virtual networks independent of physical infrastructure. Each type enhances resource utilization, flexibility, and management in computing environments.

1. Name the components used in VMware infrastructure what are benefit of virtualization?

In short, components used in a VMware infrastructure include ESXi, vCenter Server, vSphere Client, vSphere Web Client, vSphere Distributed Switch, vSphere HA, and vSphere DRS. Benefits of virtualization in VMware infrastructure include resource optimization, flexibility, scalability, improved disaster recovery, reduced downtime, centralized management, and enhanced security.