WIPRO ASSINGMENT WORK DAY -1

USER ID-28994

NAME-DIVYA JHA

TOPIC IT-INFTA INTRODUCTION

Introduction to networking devices

Networking devices are essential components that enable communication and data sharing between computers and other electronic devices within a network. These devices help create, manage, and maintain different types of networks, such as LANs (Local Area Networks) and WANs (Wide Area Networks). Common networking devices include routers, switches, hubs, modems, access points, firewalls, and more. A **router** connects different networks together, such as a home network to the internet, and directs data between them. A **switch** connects multiple devices within the same network and forwards data only to the intended recipient device, making it more efficient than a **hub**, which simply broadcasts data to all devices. A **modem** converts digital signals to analog and vice versa, allowing access to the internet over telephone or cable lines. **Access points** provide wireless (Wi-Fi) connectivity to a wired network, while **firewalls** monitor and control incoming and outgoing traffic to ensure network security. Other devices include **bridges**, which connect and filter traffic between two network segments; **gateways**, which act as translators between different network protocols; **repeaters**, which amplify signals to extend network range; and **Network Interface Cards (NICs)**, which are installed in devices to allow them to connect to a network. Together, these devices form the foundation of modern communication systems in homes, businesses, and data centers.

Different networking terms

 **Intranet**

* **Definition:** A private internal network used within an organization.
* **Purpose:** To share documents, applications, schedules, or company news securely.
* **Example:** A university’s intranet where students access exam schedules, internal emails, and learning materials.
* **Access:** Only authorized users within the organization.

 **Internet**

* **Definition:** A global network of interconnected computers and servers that allows data sharing and communication.
* **Purpose:** To access websites, social media, email, cloud services, etc.
* **Example:** Browsing websites like [www.wikipedia.org](http://www.wikipedia.org) or [www.amazon.com](http://www.amazon.com) using a web browser.
* **Access:** Public and global.

 **Email (Electronic Mail)**

* **Definition:** A method for sending and receiving digital messages over a network.
* **Purpose:** Communication, file sharing, and official correspondence.
* **Protocols Used:** SMTP (Send), IMAP or POP3 (Receive).
* **Example:** Sending an email from john@gmail.com to jane@yahoo.com using Gmail or Outlook.

 **FTP (File Transfer Protocol)**

* **Definition:** A protocol used to transfer files between computers over a network.
* **Purpose:** Uploading/downloading files from servers, website management.
* **Example:** A web developer uploads a website's HTML files to a web server using FileZilla FTP client.
* **URL Example:** ftp://ftp.example.com

 **HTTP (HyperText Transfer Protocol)**

* **Definition:** The foundation of data communication on the web, used to load web pages.
* **Purpose:** Accessing websites, transferring web content from server to browser.
* **Example:** When you type http://www.google.com in your browser, it uses HTTP to fetch and display the webpage.
* **Secure Version:** HTTPS (uses encryption for secure communication).

 **ISP (Internet Service Provider)**

* **Definition:** A company that provides access to the internet and related services.
* **Purpose:** Offers internet connection, domain registration, web hosting, etc.
* **Example:**
  + In India: **Jio**, **Airtel**, **BSNL**
  + In the US: **Comcast**, **Verizon**, **Spectrum**
*  **IP Address** – A unique identifier assigned to each device on a network.  
  Example: 192.168.1.5 (IPv4), 2001:0db8::1 (IPv6)
*  **MAC Address** – A hardware address that uniquely identifies a device on a local network.  
  Example: 00:1A:2B:3C:4D:5E
*  **Router** – A device that connects different networks and routes data between them.  
  Example: Your home Wi-Fi router connects your LAN to the internet.
*  **Switch** – A device that connects multiple devices within the same network and forwards data intelligently based on MAC addresses.  
  Example: Used in offices to connect computers to a LAN.
*  **Hub** – A basic networking device that sends data to all connected devices (less efficient than a switch).  
  Example: Used in small or outdated networks.
*  **Modem** – Converts digital signals to analog for internet access over phone or cable lines.  
  Example: DSL or cable modem provided by your ISP.
*  **Access Point (AP)** – Provides wireless access to a wired network.  
  Example: Wi-Fi access point in a classroom or café.
*  **Firewall** – A security device or software that filters incoming and outgoing traffic.  
  Example: Windows Firewall, or a hardware firewall in data centers.
*  **Gateway** – Connects different networks and translates protocols if necessary.  
  Example: A router acting as a gateway to the internet.
*  **DNS (Domain Name System)** – Translates domain names into IP addresses.  
  Example: www.google.com → 142.250.190.78
*  **DHCP (Dynamic Host Configuration Protocol)** – Automatically assigns IP addresses to devices.  
  Example: Your Wi-Fi router assigning IPs to connected phones/laptops.
*  **NAT (Network Address Translation)** – Allows multiple devices to share one public IP address.  
  Example: Used in home networks to connect multiple devices through one internet connection.
*  **VLAN (Virtual Local Area Network)** – Logically segments a physical network into separate networks.  
  Example: Separating sales and HR departments in a company network.
*  **ISP (Internet Service Provider)** – Provides internet access and related services.  
  Example: Airtel, Jio, Comcast, BSNL
*  **SSID (Service Set Identifier)** – The name of a wireless network.  
  Example: HomeWiFi\_5G, Campus\_WiFi
*  **VPN (Virtual Private Network)** – Creates a secure, encrypted connection over the internet.  
  Example: Employees using VPN to access office resources remotely.
*  **Port** – Identifies specific services or applications on a device.  
  Example: HTTP (port 80), HTTPS (port 443), FTP (port 21)
*  **Protocol** – A set of rules for data communication.  
  Example: TCP, UDP, FTP, HTTP, SMTP
*  **Packet** – A unit of data sent over a network.  
  Example: A file sent over the internet is broken into packets.

 **Latency** – The delay in data transmission across a network.  
 Example: High latency can cause lag in video calls or online games.

 **Bandwidth** – The maximum rate of data transfer in a network.  
 Example: 100 Mbps internet speed = high bandwidth.

 **FTP (File Transfer Protocol)** – Used for transferring files over a network.  
Example: Uploading website files to a server using FileZilla.

 **HTTP/HTTPS** – Protocols for accessing web pages. HTTPS is secure.  
Example: HTTP – http://example.com, HTTPS – <https://secure.com>

 **Ping** – A tool to test connectivity and measure response time.  
Example: ping google.com to check if Google is reachable.

 **Switching** – The process of directing data within the same network based on MAC addresses.  
Example: A switch forwarding a file from one computer to another on the same LAN.

 **Routing** – The process of selecting the best path for data between networks.  
Example: A router determining the fastest route to a website.

Overview of LAN and WAN technologies

Here's an overview of **LAN (Local Area Network)** and **WAN (Wide Area Network)** technologies, covering their key concepts, types, and examples:

**🖧 Local Area Network (LAN)**

**✅ Definition:**

A LAN is a network that connects computers and devices within a limited geographical area such as a home, office, or campus.

**📌 Characteristics:**

* **Short-range:** Typically spans a few meters to a few kilometers.
* **High speed:** Usually offers high data transfer rates (up to 1 Gbps or higher).
* **Private ownership:** Often managed and maintained by a single organization or individual.
* **Low latency:** Due to short distances and limited devices.

**🔧 Common LAN Technologies:**

| **Technology** | **Description** |
| --- | --- |
| **Ethernet** | Most common LAN technology; supports speeds from 10 Mbps to 100 Gbps. |
| **Wi-Fi (IEEE 802.11)** | Wireless LAN technology; commonly used in homes and offices. |
| **Token Ring (legacy)** | IBM's older LAN technology using token passing. |
| **FDDI** | Fiber Distributed Data Interface; used for backbone LANs with high reliability. |

**📶 LAN Devices:**

* Switches
* Hubs (obsolete)
* Routers (for connecting to external networks)
* Access Points (for Wi-Fi)

**🌍 Wide Area Network (WAN)**

**✅ Definition:**

A WAN connects computers and networks across large geographical areas — cities, countries, or even continents.

**📌 Characteristics:**

* **Long-range:** Spans wide geographical locations.
* **Lower speed (compared to LAN):** Typically slower due to distance and complexity.
* **Public/private ownership:** Uses both private links and public infrastructures.
* **Higher latency:** Due to longer distances and more complex routing.

**🔧 Common WAN Technologies:**

| **Technology** | **Description** |
| --- | --- |
| **Leased Lines (e.g., T1, E1)** | Dedicated private circuits; reliable but expensive. |
| **MPLS (Multiprotocol Label Switching)** | High-performance network routing for enterprise WANs. |
| **ATM (Asynchronous Transfer Mode)** | Old tech using fixed-sized cells; used in legacy systems. |
| **Frame Relay** | Legacy packet-switching tech; replaced by MPLS. |
| **Broadband (DSL, Cable)** | Used by ISPs to provide internet access. |
| **Satellite** | Used in remote areas; higher latency. |
| **5G/4G LTE** | Mobile networks capable of WAN-like connectivity. |
| **VPN (Virtual Private Network)** | Secure tunnels over the internet for private WAN access. |

**📡 WAN Devices:**

* Routers
* Modems
* Firewalls
* WAN Optimizers

**🔄 Comparison:**

| **Feature** | **LAN** | **WAN** |
| --- | --- | --- |
| **Coverage** | Local (up to a few km) | Global (hundreds to thousands of km) |
| **Speed** | High | Lower |
| **Cost** | Low | High |
| **Latency** | Low | Higher |
| **Ownership** | Private | Shared/public/private |
| **Setup** | Simple | Complex |

IPv4 and IPV6

| **Feature** | **IPv4** | **IPv6** |
| --- | --- | --- |
| **Address Size** | 32-bit | 128-bit |
| **Address Format** | Decimal (e.g., 192.168.0.1) | Hexadecimal (e.g., 2001:db8::1) |
| **Total Addresses** | ~4.3 billion | ~340 undecillion |
| **Header Complexity** | Simple | More complex |
| **Configuration** | Manual or DHCP | Auto-config (Stateless) |
| **Security** | Not built-in | Built-in (IPSec) |
| **NAT Required?** | Often yes | Not required |
| **Broadcasting** | Supported | Not supported |
| **Deployment** | Widely used | Still being adopted |

Datacenter overview

A **Data Center** is a **facility** that houses computing resources such as servers, storage systems, networking equipment, and infrastructure to **store, manage, process, and distribute data**.

Think of it as the “brain” of IT operations — running apps, storing big data, supporting websites, cloud services, etc.

**🧩 Core Components of a Data Center:**

| **Component** | **Description** |
| --- | --- |
| **Servers** | Powerful computers that run applications and services. |
| **Storage Systems** | For storing massive amounts of data (e.g., HDDs, SSDs, SAN, NAS). |
| **Networking Equipment** | Routers, switches, firewalls — manage traffic and security. |
| **Power Supply** | Redundant power systems including UPS (Uninterruptible Power Supply) and generators. |
| **Cooling Systems** | HVAC systems and cooling units to keep hardware at optimal temperature. |
| **Physical Security** | Cameras, access control, biometric scanners to secure the facility. |
| **Cabling** | Structured cables for data and power connectivity. |

**☁️ Types of Data Centers:**

| **Type** | **Description** |
| --- | --- |
| **Enterprise Data Center** | Built and operated by companies for internal use. |
| **Colocation (Colo)** | Rent space and infrastructure in a third-party facility. |
| **Cloud Data Center** | Operated by cloud providers (e.g., AWS, Azure, Google Cloud). |
| **Edge Data Center** | Smaller facilities located closer to end-users to reduce latency. |

**⚙️ Key Characteristics:**

* **High Availability (HA):** Redundancy in power, networking, and hardware to minimize downtime.
* **Scalability:** Easy to add more servers or storage as demand grows.
* **Security:** Both **physical** and **cybersecurity** are top priorities.
* **Energy Efficiency:** Focus on green technologies to reduce power usage (measured using PUE – Power Usage Effectiveness).

**🌐 Tier Classification (Uptime Institute):**

| **Tier** | **Description** | **Uptime** |
| --- | --- | --- |
| **Tier I** | Basic, non-redundant | ~99.671% |
| **Tier II** | Redundant components | ~99.741% |
| **Tier III** | Concurrently maintainable | ~99.982% |
| **Tier IV** | Fault tolerant | ~99.995% |

**📈 Common Use Cases:**

* Hosting websites and applications
* Cloud computing and SaaS platforms
* Big data processing and storage
* Backup and disaster recovery
* Enterprise email and collaboration tools

Server form factor

**Server form factor** refers to the **physical size, shape, and configuration** of a server. Different form factors are optimized for different environments (like space, performance, cooling, scalability, etc.).

**📦 Main Types of Server Form Factors:**

| **Form Factor** | **Description** | **Pros** | **Use Case** |
| --- | --- | --- | --- |
| **Tower Server** | Looks like a regular desktop PC (vertical case) | - Low cost - Easy setup | Small businesses, entry-level IT |
| **Rack Server** | Flat and wide, designed to be mounted in a server rack (e.g., 1U, 2U, etc.) | - Space-efficient - Scalable | Data centers, enterprise IT |
| **Blade Server** | Slim servers (blades) that slide into a chassis | - High density - Centralized power & cooling | Large-scale computing, virtualization |
| **Hyper-converged / Modular Server** | Modular design that combines storage, networking, and compute | - Flexible - Easily scalable | Cloud infrastructure, edge computing |

**What is a Server Management Portal?**

A **server management portal** is a web-based or network-based interface that allows IT admins to monitor, manage, and troubleshoot servers **remotely**, even if the server is **powered off** or the **OS is unresponsive**.

These tools are often called **Out-of-Band Management** interfaces.

**🔧 Popular Server Management Technologies:**

| **Name** | **Vendor** | **Full Form** | **Key Use** |
| --- | --- | --- | --- |
| **IPMI** | Industry Standard | Intelligent Platform Management Interface | Base-level hardware management |
| **iLO** | HPE | Integrated Lights-Out | HPE server remote management |
| **iDRAC** | Dell | Integrated Dell Remote Access Controller | Dell server remote management |
| **IMM/XClarity** | Lenovo/IBM | Integrated Management Module | Lenovo server management |
| **BMC** | General term | Baseboard Management Controller | Hardware chip used in all of the above |

**📌 Common Features of These Portals:**

| **Feature** | **Description** |
| --- | --- |
| **Remote KVM** | View the server’s screen, keyboard, and mouse remotely |
| **Power control** | Power on/off or reboot the server remotely |
| **Hardware monitoring** | CPU temp, fan speed, power usage, etc. |
| **System logs** | View hardware events or error logs |
| **Firmware updates** | Update BIOS, firmware, and drivers |
| **Virtual media** | Mount ISOs over the network for OS installs |
| **User access control** | Set roles and permissions for admins |

**server management portal(ipmi/ilo,iDrac)**

**Details on Each Platform:**

**1. IPMI (Intelligent Platform Management Interface)**

* **Standardized** protocol supported by most vendors.
* Managed by the **BMC**.
* Basic functionality.
* CLI-based and sometimes older UI.
* Good for cross-platform compatibility.

**2. iLO (Integrated Lights-Out) – HPE**

* Powerful web-based UI with advanced features.
* Available in multiple editions (iLO Standard, iLO Advanced).
* Secure remote console, health monitoring, scripting via REST API.

**3. iDRAC (Integrated Dell Remote Access Controller) – Dell**

* Built into Dell PowerEdge servers.
* iDRAC9 (latest as of 2025) offers virtual console, lifecycle controller, telemetry, and RESTful API.
* Comes in Basic and Enterprise versions.

**🔒 Security Considerations:**

* Always **change default credentials**.
* Use **HTTPS** and **firewall rules**.
* Keep **firmware updated** to avoid vulnerabilities.
* Disable if unused to minimize attack surface.

**✅ Use Case Scenarios:**

| **Situation** | **Why It's Useful** |
| --- | --- |
| Server not booting | Use remote KVM to troubleshoot BIOS or OS |
| OS crash | Reboot or reinstall using virtual media |
| Hardware failure | Get alerts before things break completely |
| No on-site staff | Manage from anywhere in the world |

Server Events

**🧭 Common Types of Server Events:**

| **Event Type** | **Description** | **Example** |
| --- | --- | --- |
| **Power Events** | Changes in power state | Power on/off, reboot, power failure |
| **Hardware Events** | Hardware health or failure | CPU overheating, memory failure, disk failure |
| **Network Events** | Network interface status | Link up/down, MAC/IP conflict, NIC failure |
| **Login/Access Events** | User logins or authentication attempts | Successful login, failed login, unauthorized access |
| **System Boot/Shutdown Events** | OS startup or shutdown | OS loaded, shutdown initiated |
| **Firmware/BIOS Events** | Firmware activity or updates | BIOS update started/successful |
| **Virtual Media Events** | ISO or remote media mount/unmount | ISO mounted via iDRAC/iLO |
| **Environmental Events** | Server environment alerts | High temperature, fan failure, low voltage |
| **Storage Events** | Disk or RAID alerts | Disk SMART errors, RAID rebuild |
| **Security Events** | Security policy or intrusion detection | Port scan detected, policy violation |

Basics of storage(NAS,DAS and SAN)

| **Type** | **Full Form** | **Connected To** | **Protocols** | **Best For** |
| --- | --- | --- | --- | --- |
| **DAS** | Direct Attached Storage | Directly to one server | SATA, SAS, NVMe | Simple, local storage |
| **NAS** | Network Attached Storage | Network (via Ethernet) | NFS, SMB/CIFS | File sharing across multiple users |
| **SAN** | Storage Area Network | High-speed network | iSCSI, Fibre Channel | High-performance, block-level access |

In enterprise IT, storage systems are essential for managing and accessing data efficiently. The three primary types of storage architectures are **Direct Attached Storage (DAS)**, **Network Attached Storage (NAS)**, and **Storage Area Network (SAN)**. **DAS** refers to storage devices that are directly connected to a single server, such as internal hard drives or external USB drives. It offers high-speed access for that specific server but lacks the ability to share data across a network, making it suitable for personal use or small-scale server setups. In contrast, **NAS** is a dedicated file storage device connected to a standard network via Ethernet, allowing multiple users and devices to access and share files over protocols like NFS or SMB. NAS is ideal for file sharing, data backups, and centralized storage in office or home environments. Lastly, **SAN** is a high-performance, high-speed network that provides block-level storage to multiple servers. It uses technologies like Fibre Channel or iSCSI and is commonly used in large data centers for applications that require fast data access, such as databases and virtual machines. SAN offers excellent scalability and performance but is more complex and expensive to set up. Each storage type has its own strengths and is chosen based on performance needs, cost, scalability, and sharing requirements.

comparing fibre channel,iscsi, and fibre channel over ethernet

| **Feature** | **Fibre Channel (FC)** | **iSCSI** | **Fibre Channel over Ethernet (FCoE)** |
| --- | --- | --- | --- |
| **Protocol Type** | Fibre Channel | IP-based (SCSI over TCP/IP) | Fibre Channel encapsulated over Ethernet |
| **Network Type** | Dedicated Fibre Channel network | Standard Ethernet/IP network | High-speed Ethernet network (DCB required) |
| **Speed** | 8/16/32 Gbps | 1/10/25 Gbps (depending on Ethernet) | 10/25/40+ Gbps |
| **Latency** | Very low | Higher than FC | Comparable to FC (with right setup) |
| **Cost** | High (dedicated hardware) | Low (uses existing Ethernet) | Medium (needs DCB switches) |
| **Complexity** | High | Low to Medium | Medium |
| **Infrastructure** | Separate SAN (FC switches, HBAs) | Existing LAN with NICs | Converged LAN/SAN (DCB switches, CNA cards) |
| **Use Case** | Large enterprise SANs | SMBs, virtualization, low-budget setups | Data centers wanting convergence |
| **Scalability** | Excellent | Good | Good |
| **Management** | Specialized tools | Standard IP tools | Specialized + Ethernet tools |

**Fibre Channel (FC)**, **iSCSI**, and **Fibre Channel over Ethernet (FCoE)** are three widely used protocols for transferring block-level data between servers and storage in Storage Area Networks (SANs). **Fibre Channel** is a high-performance, low-latency protocol that operates over a dedicated Fibre Channel network using special switches and cables. It is highly reliable and fast (up to 32 Gbps or more) but requires a separate, expensive infrastructure, making it suitable for large enterprise environments. In contrast, **iSCSI (Internet Small Computer Systems Interface)** runs over standard Ethernet networks and uses IP protocols to transmit SCSI commands. This makes iSCSI more cost-effective and easier to implement, especially in small to medium-sized organizations, though it may introduce higher latency compared to FC. **Fibre Channel over Ethernet (FCoE)** is a hybrid solution that encapsulates Fibre Channel frames within Ethernet packets, allowing FC traffic to travel over modern high-speed Ethernet networks (typically 10 Gbps or higher). It reduces the need for separate cabling and hardware, offering a balance between performance and cost. However, FCoE still requires special data center bridging (DCB)-capable switches to ensure reliable, lossless transmission. In summary, **FC** offers the best performance but is expensive, **iSCSI** is more affordable and uses existing infrastructure, and **FCoE** provides a middle-ground solution by combining Fibre Channel performance with Ethernet flexibility.