IT Infrastructure

Agenda – Day 1

- Introduction to Networking Devices
- Overview of LAN and WAN technologies
- IPv4 and IPv6
- Datacenter Overview
- Server form factor
- Server Management portal (IPMI/iLO, iDrac)
- Server Events
- Basics of storage (NAS, DAS and SAN)
- Comparing Fibre Channel, iSCSI, and Fibre Channel over Ethernet

Agenda – Day 2

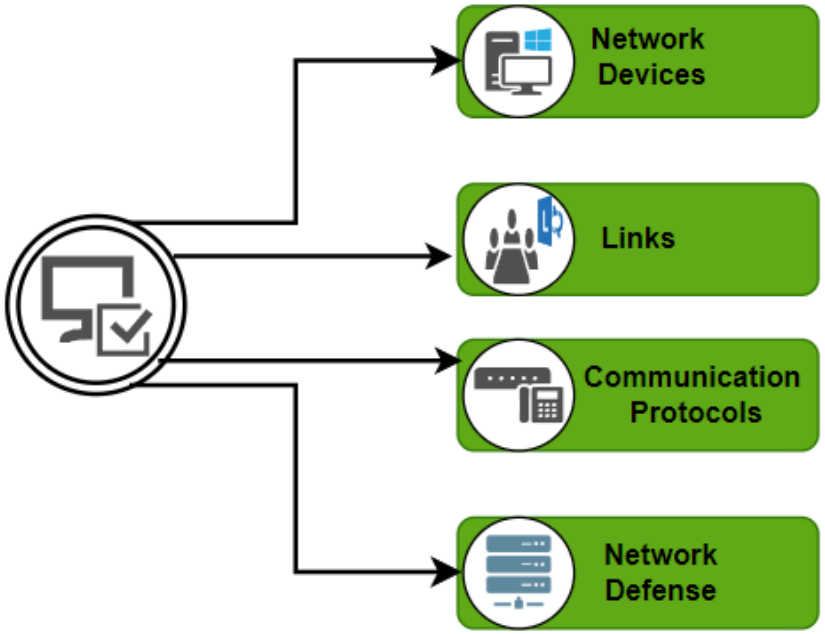
- Concept of RAID
- Introduction to Operating systems (Server and Client)
- Concept of Domain and Workgroup
- File Systems (FAT, NTFS, ReFS, EXT3, EXT4 etc)
- File system management
- Installing Operating system (Windows 10, Server 2016, Linux
- Installing OS using management Console
- Firewall (Hardware and Software)

What is a Computer Network?

- A computer network is a system that connects many independent computers to share information (data) and resources.
- The integration of computers and other different devices allows users to communicate more easily.
- A network connection can be established using either cable or wireless media.
- Hardware and software are used to connect computers and tools in any network.

Key Components of a Computer Network

- A computer network is made up of two main parts:
  - **Devices** (called nodes) &
  - **Connections** (called links)
- The links connect the devices to each other.



- The rules for how these connections send information are called communication protocols.
- The starting and ending points of these communications are often called ports.

Port Numbers

- In networking, ports are categorized primarily based on their port numbers, which range from 0 to 65535.
- These ports are divided into three main categories as defined by the Internet Assigned Numbers Authority (**IANA**):
  - **Well-Known Ports** (0 – 1023)
  - **Registered Ports** (1024 – 49151)
  - Dynamic/Private/**Ephemeral Ports** (49152 – 65535)

Port Numbers – Well-Known Ports

- **Ranges** from 0 – 1023
- **Used by**: Common system or well-known services.
- **Reserved for**: Privileged services and processes.
- **Examples**:
  - 20, 21 – FTP (File Transfer Protocol)
  - 22 – SSH (Secure Shell)
  - 23 – Telnet
  - 25 – SMTP (Simple Mail Transfer Protocol)
  - 53 – DNS (Domain Name System)
  - 80 – HTTP (HyperText Transfer Protocol)
  - 443 – HTTPS (HTTP Secure)

Port Numbers – Registered Ports

- **Ranges** from 1024 – 49151
- **Used by:** User processes or applications.
- Registered with IANA for specific services by software developers.
- Examples:
  - 1433 – Microsoft SQL Server
  - 3306 – MySQL Database
  - 3389 – Microsoft RDP (Remote Desktop Protocol)
  - 8080 – HTTP alternative port (often used by web servers)

Port Numbers – Dynamic/Private/Ephemeral Ports

- **Ranges** from 49152 – 65535
- **Used by**: Temporary connections, usually client-side.
- Assigned dynamically by the operating system when an application requests a network connection.
- **Examples**:
  - Any port in this range used for NAT (Network Address Translation), temporary communication, or client-side connections in TCP/UDP communications.

Networking devices

- Networking devices are hardware components used to connect computers, printers, phones, cameras, servers, and other devices to a network, enabling them to communicate and share data.

- These devices perform functions like:
  - *Routing data* to the correct destination
  - *Filtering* or *managing* traffic
  - *Connecting* different types of networks

Common Networking Devices

- *Router*
- *Switch*
- Hub
- *Modem*
- *Access Point*
- *Firewall*
- *Gateway*
- *Network Interface Card (NIC)*
- Repeater
- Bridge

Router

- Connects **multiple networks** (e.g., LAN to the Internet).
- Routes data packets based on **IP addresses**.
- Determines **best path for data** to reach its destination.
- Often includes **Wi-Fi functionality** in home routers.
- Offers basic security features like **firewall** and **NAT** (Network Address Translation).
- Supports **DHCP** to assign IP addresses to devices.
- Has **WAN** and **LAN** ports for external and internal network connections.
- Maintains a **routing table** to manage data flow.
- Can be configured via **web interface** or **CLI**.

Switch

- Connects multiple devices within the **same LAN**.
- Forwards data only to the **specific device** (MAC address) that needs it.
- Maintains **a MAC address table** to map ports to devices.
- Operates at **Layer 2** (Data Link Layer) of the OSI model (some at Layer 3 with routing capability).
- Provides **faster and more efficient data** transmission than a hub.
- Has **multiple Ethernet ports** (e.g., 8, 24, 48 ports).
- Used in **offices, data centers**, and **enterprise** networks to interconnect devices.
- May be managed or unmanaged:
  - **Managed**: configurable, supports VLANs, monitoring, etc.
  - **Unmanaged**: plug-and-play, no configuration needed.
- Reduces network collisions and **improves performance** over hubs.

Hub

- Connects **multiple devices in a LAN**.
- **Broadcasts incoming data** to all ports, regardless of destination.
- **Does not store MAC** addresses or make intelligent forwarding decisions.
- Operates at **Layer 1 (Physical Layer)** of the OSI model.
- Slower and less efficient compared to switches.
- Typically has **multiple Ethernet ports** (e.g., 4, 8, 16).
- **Unmanaged device** – no configuration required.
- **Rarely used today**, mostly replaced by switches.
- Useful in basic setups or labs for understanding network behavior.

Modem

- Modem = **Modulator + Demodulator**.
- Converts **digital signals** from a computer to **analog signals** for transmission over phone/cable lines.
- Connects a **home** or **office** network to the Internet via an ISP.
- Typically has one port for the ISP line and one for connecting to a router or computer.
- Works at the **Physical Layer (Layer 1)** of the OSI model.
- **Does not manage internal network** traffic – only handles the internet connection.
- **Required for internet** access in homes and small businesses.

Access Point

- Provides **wireless connectivity** to devices within a network.
- Connects to a wired network (e.g., via Ethernet) and **creates a Wi-Fi network**.
- **Acts as a bridge** between wireless clients and wired LAN.
- **Extends Wi-Fi** coverage in large areas (offices, campuses, hotels).
- Operates at **Layer 2** (Data Link Layer) of the OSI model.
- Supports **multiple devices** simultaneously (smartphones, laptops, etc.).
- Not the same as a router — it **doesn't route traffic** between networks.
- Used to **improve scalability, range**, and **performance** of wireless networks.

Firewall

- **Monitors and controls** incoming and outgoing network traffic.
- Acts as a **barrier** between trusted and untrusted networks (e.g., LAN and Internet).
- Uses **predefined rules** to allow or block data packets.
- Filters traffic based on **IP address, port number, protocol, or content.**
- Operates primarily at **Layer 3 (Network)** and **Layer 4 (Transport)** of the OSI model.
- Protects against **unauthorized access, malware, and attacks**.
- **Configurable by administrators** for custom security policies.

Gateway

- Connects two different networks that use different protocols.
- Acts as a translator or protocol converter between dissimilar systems.
- Enables communication between LAN and WAN, or enterprise network and internet.
- Operates at all seven layers of the OSI model (depending on implementation).
- *Commonly used to connect internal networks to external networks (e.g., the Internet).*
- Can include routing, firewall, and NAT functionality.
- Can be implemented as hardware, software network as an entry/exit point, or cloud-based service.
- In home/office networks, the router often acts as the default gateway.

Network Interface Card (NIC)

- Enables a device (computer, printer, server, etc.) to connect to a network.
- Provides a physical interface (e.g., Ethernet port or wireless adapter).
- Can be wired (Ethernet NIC) or wireless (Wi-Fi NIC).
- Has a unique MAC (Media Access Control) address for identification.
- Operates at Layer 2 (Data Link Layer) and interfaces with Layer 1 (Physical Layer).
- Can be integrated into the motherboard or added as a separate expansion card.
- Essential for network communication in desktops, laptops, and servers.
- Transmits and receives data packets over the network.
- Supports various speeds like 10/100/1000 Mbps or 10 Gbps and beyond.
- Required for both LAN and Internet access.

Repeater

- Amplifies and retransmits network signals to extend the range.
- Used to boost weak or degraded signals in a network.
- Helps maintain signal strength over long distances.
- Connects two network segments using the same protocol.
- Operates at Layer 1 (Physical Layer) of the OSI model.
- Has no filtering or addressing capabilities — just regenerates signals.
- Common in wired (Ethernet) and wireless (Wi-Fi extender) networks.
- Useful when cabling exceeds the standard-length limit (e.g., 100 meters for Ethernet).
- Does not reduce network traffic or collisions — just extends coverage.
- Ideal for simple network expansion in homes or small offices.

Bridge

- Connects and filters traffic between two or more LAN segments.
- Forwards data based on MAC addresses.
- Maintains a MAC address table to determine which segment to forward traffic to.
- Helps reduce network traffic and collisions by dividing large networks.
- Operates at Layer 2 (Data Link Layer) of the OSI model.
- Connects networks using the same protocol (unlike a gateway).
- Can segment a busy network to improve performance and efficiency.
- Typically has two or more ports for connecting network segments.
- Useful in legacy or small networks before switches became common.
- Can be implemented as hardware or software (e.g., in virtual environments).


That's all Folks!