[CNet - F25]

Computer Networks

</Lecture-01/>

FUNDAMENTALS OF COMPUTER NETWORKS

Week 2 - (14 SEPT 2025)

Today's agenda

01

BASICS OF NETWORKING

Definition and Importance of computer networks.

02

TYPES OF NETWORKS

PAN, LAN, MAN, and WAN

03

NETWORK TOPOLOGIES

RING, STAR, MESH, BUS, AND HYBRID

04

OSI MODEL

Open Systems & OSI Layers Model

05

LEARNING ACTIVITIES

Interactive Discussion, Real-World Case Studies, DEMO Labs, Quiz#1, Assignment#1

06

Q & A Session

Q&A session for students to ask questions about today's presentation.

[REASONING BEHIND]

</// WHAT? & WHY? //>

> What is a computer networks?
>
> Why Do We Need it?
>
> Why should you take this course, then?

INTEREST

DEFINITION & IMPORTANCE

Definition: A computer network is a collection of interconnected devices that share resources and data.

It allows data exchange between devices such as computers(Clients), servers, and network hardware.

Importance:

- ✓ **Facilitates communication:** Email, social media, and real-time messaging rely on networks.
- ✓ **Resource sharing:** Devices (e.g., printers) and data can be shared across a network.
- ✓ **Enhances efficiency:** Enables collaboration in real-time, enhancing productivity.
- ✓ **Provides scalability:** Networks grow with the organization's needs.

</ Why Should All Departments Enrol ? />

NETWORK ENGINEERS

Needs to **master the foundation** of network design, Devices, setup, configurations, and security. Which is vital for managing modern infrastructure.

SOFTWARE ENGINEERS

Understanding networks is very crucial for software developers, as most rely on network communication and integration with infrastructure.

INFO MANAGEMENT

Be prepared to manage digital infrastructures, select and procure the right equipment, and set up systems

TYPES OF NETWORKS

- **A Personal Area Network (PAN)** is designed for short-range communication between personal devices, such as connecting a phone to a headset via Bluetooth. PANs usually operate within a range of **1-10 meters**, providing low-power, short-distance connectivity for personal device interactions.

- **A Local Area Network (LAN)** connects devices within a small geographic area, such as a building, office, or campus. It typically operates within a range of up to **100 meters**. LANs offer high-speed connections, often reaching **1 Gbps or more**, making them ideal for homes, offices, or schools where devices are closely situated.

TYPES OF NETWORKS

- **A Metropolitan Area Network (MAN)** serves as a middle ground between LAN and WAN, connecting networks across a city or large campus. It can cover up to **50 kilometers** and offers faster speeds than a WAN while still providing broader coverage than a LAN. MANs are often used for city-wide Wi-Fi or connecting large institutions.

- **A Wide Area Network (WAN),** on the other hand, covers a much larger geographic area**, connecting multiple LANs across cities, countries, or even globally**. WANs can span thousands of kilometers, providing long-distance communication, such as the **InterNet**. However, they tend to be slower than LANs due to the vast distances involved.

NETWORK TOPOLOGIES

- **Ring:** Each node connects to two others forming a circular pathway. Data travels in one direction.
- **Star:** All nodes are connected to a central device(s). Easy to manage and expand.
- **Bus:** All devices share a single communication line. Simple but can be less reliable.
- **Mesh:** Every node connects directly to every other node. Highly reliable but expensive.
- **Hybrid:** Combination of two or more topologies. Flexible and scalable.

PROPRIETARY SYSTEMS

- A proprietary system is a system that uses technologies controlled and kept private by a specific vendor, restricting compatibility and communication.

- **Key Challenges:**
  - Proprietary systems hinder communication between different technologies.
  - Each vendor's system is unique, preventing interoperability with others.
- **Example:**
  - Early computer networks were vendor-specific, meaning systems from different manufacturers couldn't communicate.

SOLUTION

- Interoperability refers to the ability of software and hardware from multiple machines, and often from multiple vendors, to communicate effectively.

- **Importance:**
  - Seamless communication between devices and systems is critical for the growth of global networking.
  - It enables collaboration across different systems, regardless of their underlying vendor technologies.
- **Early Networking Issues:**
  - Without interoperability, organizations struggled to connect different vendor products in a single environment.

</ ISO & OSI MODEL />

- **ISO's Role**
  - The International Organization for Standardization (ISO) took the lead in developing a standardized network model to support open systems.
- **OSI Model Overview:**
  - Open Systems Interconnection (OSI) Model is a conceptual framework for understanding network interactions in seven layers.
  - Each layer serves a specific function and interacts with the layers above and below it, creating a universal blueprint for network communication.
- **Layers & Technique:**
  - **A**pplication, **P**resentation, **S**ession, **T**ransport, **N**etwork, **D**ata link, **P**hysical
  - **A**ll **P**eople **S**eems **T**o **N**eed **D**ata **P**rotection.

OSI LAYERS MODEL

7. Application	End-user services and application protocols.
6. Presentation	Data translation and encryption.
5. Session	Manages sessions between applications.
4. Transport	Reliable data transfer; TCP/UDP protocols.
3. Network	Routing data packets; IP addressing.
2. Data Link	Node-to-node data transfer; MAC addresses.
1. Physical	Physical connection; cables and switches.

SUMMARY

- In this second week, we covered the foundational concepts of networking, including the definition and importance of computer networks. We explored various types of networks—PAN, LAN, MAN, and WAN—and discussed their characteristics. We then examined different network topologies such as star, ring, mesh, bus, and hybrid topologies, highlighting their advantages and disadvantages.

- Finally, we introduced the OSI model as a crucial framework for understanding how different networking protocols interact across seven distinct layers, each with specific functions and associated protocols or devices.

Next

FUNDAMENTALS
Continue...

Today's agenda

01

NETWORK PROTOCOLS

Understanding Network Protocols

02

NETWORK PORTS

Understanding Ports and their Roles

03

NETWORK DEVICES

Network Devices Overview

04

NETWORK CONNECTIONS

Wired vs. Wireless Connections

05

LEARNING ACTIVITIES

Interactive Discussion, Real-World Case Studies, DEMO Labs, Quiz#1, Assignment#2

06

Q & A Session

Q&A session for students to ask questions about today's presentation.

NETWORK PROTOCOLS

- **Definition:** A network protocol is a set of rules and conventions for communication between network devices. Protocols determine how data is transmitted, formatted, and processed.

- **Importance:** Protocols ensure reliable data exchange, error detection, and efficient use of network resources.

- **Types of Protocols:**
  - **Communication Protocols:** TCP/IP, UDP, FTP, HTTP/HTTP,...
  - **Routing Protocols:** Static, Default, OSPF, BGP, EIGRP.,...
  - **Network Management Protocols:** SNMP, ICMP,...

NETWORK PORTS

- **Definition:** A network port is a logical point where network communication begins and ends. Ports are used to identify specific processes or services on a host. They serve as communication endpoints for devices within a network.

- **Purpose of Ports:**
  - They allow multiple services (e.g., web browsing, email) to run simultaneously on a device without confusion.
  - Each service or protocol communicates using a specific port number.
  - Ports help organize data streams and ensure that the correct application processes the right data.

NETWORK PORTS

- **Port Numbers and Their Roles:**
  - **Well-Known Ports (0–1023):** Reserved for system or widely-used services (e.g., HTTP, FTP).
  - **Registered Ports (1024–49151):** Assigned to user processes or services.
  - **Dynamic/Private Ports (49152–65535):** Temporarily used by client applications for communication.

- **Why Are Ports Important?**
  - Ports facilitate organized data flow across networks, ensuring that incoming and outgoing data packets are directed to the correct application.

  - Network engineers must understand port usage to configure firewalls, enable services, and troubleshoot connectivity issues.

[PORTS]

<// Common Network Ports //>

PORT	SERVICE/PROTOCOL	DESCRIPTION/ROLE
20, 21	FTP	Used for transferring files between a client and a server.
22	SSH	Provides secure remote login and command execution.
23	Telnet	Unsecured remote command-line interface.
25	SMTP	Used to send emails between servers.
53	DNS	Resolves domain names to IP addresses.
67, 68	DHCP	Automatically assigns IP addresses to devices.
80	HTTP	Standard for web traffic (unencrypted).
110	POP3	Retrieves email from a server.
123	NTP	Network Time Protocol (NTP), used for time sync.
443	HTTPS	Encrypted web traffic for secure communications.
389	LDAP	Used for directory services and authentication.
445	SMB	Provides file sharing and printing services over a network.
161, 162	SNMP	Simple Network Management Protocol

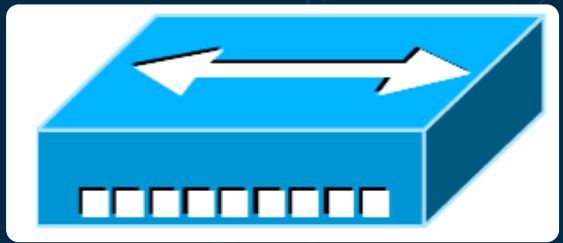
</ [HUB] NETWORK DEVICES />

- **Description:** A hub is a basic networking device that connects multiple Ethernet devices, making them act as a single network segment. Hubs operate at Layer 1 (Physical Layer) of the OSI model.

- **Functionalities:**
  - Connects multiple devices within a local area network (LAN).
  - Broadcasts incoming data packets to all connected devices.
  - Simple and inexpensive solution for small networks.

HUB Image

HUB Symbol



</ [SWITCH] NETWORK DEVICES />

- **Description:** A switch is an intelligent device that connects multiple devices within a LAN and uses MAC addresses to forward data only to the destination device. It operates at Layer 2 (Data Link Layer) of the OSI model.

- **Functionalities:**
  - Learns and maintains a MAC address table for efficient data forwarding.
  - Reduces network collisions by creating separate collision domains for each port.
  - Supports Virtual Local Area Networks (VLANs) for network segmentation.
  - Can perform basic network management tasks, such as traffic prioritization.

Switch Image

Switch Symbol

</// [ROUTER] NETWORK DEVICES //>

- **Description:** A router connects different networks and routes data packets between them using IP addresses. It operates at Layer 3 (Network Layer) of the OSI model.

- **Functionalities:**
  - Traffic Routing & Path Selection (Routes between networks, path selection, dynamic routing protocols)
  - Network Address Translation (NAT) (Allows multiple devices to share a public IP).
  - Traffic Filtering & Security (ACLs, packet filtering).
  - Internetwork Communication & Packet Forwarding (Enables communication between networks, packet switching).
  - Quality of Service (QoS) & Traffic Management (Manages bandwidth, prioritizes traffic).

Router Image

Router Symbol

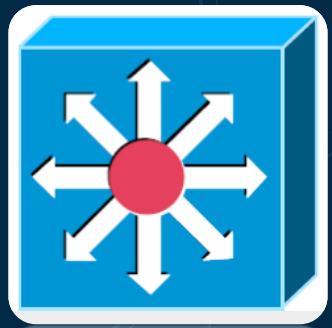
</ [BRIDGE] NETWORK DEVICES />

- **Description:** A bridge connects two or more network segments, allowing them to function as a single network. It operates at Layer 2 (Data Link Layer) of the OSI model.

- **Functionalities:**
  - Filters traffic by examining MAC addresses.
  - Reduces collisions by dividing collision domains.
  - Can connect different types of networks (e.g., wired and wireless).

Bridge Image

Bridge Symbol



</ [GATEWAY] NETWORK DEVICES />

- **Description:** A gateway is a device that connects two different networks and translates communications between them. It can operate at multiple layers of the OSI model, depending on its function.
- **Functionalities:**
  - Acts as a "gate" between two networks with different protocols.
  - Translates data formats and protocols for interoperability.
  - Can provide firewall and security functions.

Gateway Image

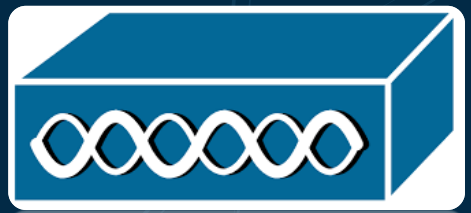
Gateway Symbol

</ [ACCESS POINT] NETWORK DEVICES />

- **Description:** An access point is a device that allows wireless devices to connect to a wired network using Wi-Fi or other wireless standards. It operates at Layer 2 (Data Link Layer) of the OSI model.
- **Functionalities:**
  - Extends the coverage area of a wired network by providing wireless connectivity.
  - Connects multiple wireless devices to a wired LAN.
  - Can provide network security features such as WPA/WPA2 encryption.

Access-Point Image

Access-Point Symbol



</ [REPEATER] NETWORK DEVICES />

- **Description:** A repeater is a device used to extend the range of a network by regenerating and amplifying signals. It operates at Layer 1 (Physical Layer) of the OSI model.
- **Functionalities:**
  - Amplifies and retransmits signals to cover longer distances.
  - Useful for extending wired or wireless networks beyond their normal limits.

Repeater Image

Repeater Symbol

</ [FIREWALL] NETWORK DEVICES />

- **Description:** A firewall is a security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It operates primarily at Layer 3 (Network Layer) and Layer 4 (Transport Layer) of the OSI model.
- **Functionalities:**
  - Filters traffic based on IP addresses, ports, and protocols.
  - Can act as a barrier between internal networks and untrusted external networks (e.g., the internet).Enforces security policies for network communication.
  - Protects against unauthorized access and potential threats.

Firewall Image

Firewall Symbol

</ [MODEM] NETWORK DEVICES />

- **Description:** A modem (modulator-demodulator) converts digital signals from a computer into analog signals for transmission over telephone or cable lines and vice versa.
- **Functionalities:**
  - Provides internet connectivity by modulating and demodulating signals.
  - Converts digital data to analog for transmission (and back to digital).
  - Enables devices to communicate over long-distance networks like the internet.

[CNet-F25]

</// NETWORK CONNECTIONS //>

ASSIGNMENT

[CNet-F25]

</THANK YOU!/>

“For I know the plans I have for you," declares the Lord, "plans to prosper you and not to harm you, plans to give you hope and future.”

Jeremiah 29:11