Introduction to Computer Networks, Protocol Layers: Computer Networks and the Internet, What is Internet? The network Edge, The Network Core, Delay, Loss, and Throughput in Packet-Switched Networks, Protocol Layers and their Service Models.

*****

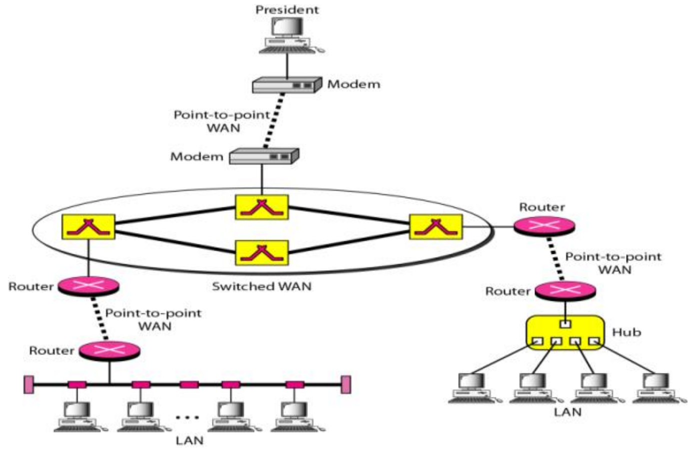
Introduction to Computer Networks:

Computer Networks:

- Computer networks are created by different entities. Standards are needed so that these heterogeneous networks can communicate with one another.
- The two best-known standards are the OSI model and the Internet model.
- The OSI (Open Systems Interconnection) model defines a seven-layer network;
- The Internet model defines a five-layer network.

Interconnection of Networks: Internetwork

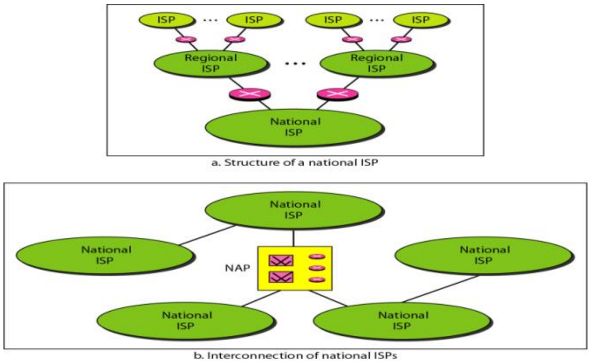
- Today, a LAN, a MAN, or a LAN is connected to one another as shown below.
- When two or more networks are connected, they become an internetwork, or internet.



The Internet:

- An internet (note the lowercase letter i) is two or more networks that can communicate with each other.
- The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.

- So the Internet is a vast, interconnected network of networks that enables global communication. It is based on the TCP/IP protocol suite and operates using packet-switching technology. The Internet provides services such as web browsing, email, video streaming, and cloud computing.
- The end users who want Internet connection use the services of Internet service providers (ISP).
- There are international service providers, national service providers, regional service providers, and local service providers as shown below.



a. Structure of a national ISP

b. Interconnection of national ISPs

Network Edge:

The network edge is where devices like computers, smart phones, and IoT gadgets interact with the Internet. It consists of:

1. End Systems (Hosts)
2. Access Networks
3. Physical Media

1. End Systems (Hosts)

End systems, also known as hosts, are the devices that run network pplications. These include:

- Personal computers (PCs, laptops, workstations)
- Mobile devices (smart phones, tablets)
- Servers (hosting websites, cloud services, applications)
- Internet of Things (IoT) devices (smart TVs, smart watches, sensors, etc.)

Types of End Systems:

- Clients: Devices that request services from servers (e.g., web browsers requesting web pages).
- Servers: Powerful machines that store and provide resources (e.g., web servers, email servers).
- Peer-to-Peer (P2P) Systems: Some end systems act as both clients and servers in a decentralized way (e.g., BitTorrent, Skype).

2. Access Networks

The access network connects end systems to the first router (edge router) in the ISP's network. Different types of access networks include:

Wired Access Networks

- DSL (Digital Subscriber Line): Uses telephone lines, up to 100 Mbps.
- Cable Broadband: Uses coaxial cable, 100 Mbps – 1 Gbps.
- Fiber-Optic (FTTH - Fiber To The Home): High-speed data transmission, 1 Gbps – 10 Gbps.

Wireless Access Networks

- Wi-Fi (Wireless LANs): Uses radio waves within a local area.
- Cellular Networks (4G, 5G): Uses mobile towers to connect users to the Internet over long distances.

3. Physical Media

The physical media refers to the actual materials that transmit data signals:

- Twisted-Pair Copper Wires: Used in telephone lines and Ethernet cables.
- Coaxial Cable: Used for cable Internet connections.
- Fiber Optic Cable: High-speed, long-distance communication.
- Wireless (Radio, Microwave and Satellite): Used for mobile networks, satellite communication, and Wi-Fi.

The Network Core:

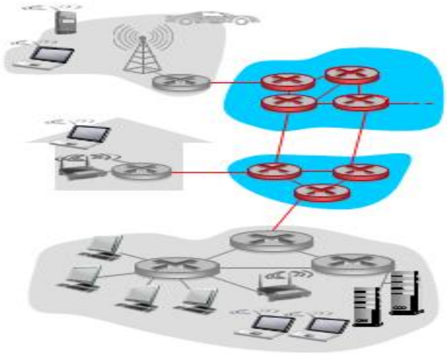
Introduction to The Network Core

The network core is the central part of a network that connects end systems (hosts) and routes data across the network. It consists of routers, switches, and links that handle packet transmission between different devices.

Key Functions of the Network Core:

- Moves data from source to destination efficiently.
- Uses routing and forwarding mechanisms.
- Manages congestion and optimizes network performance.

The **network edge** consists of devices like computers, smartphones, and IoT devices, while the **network core** is the backbone that connects everything together.



Key Functions of the Network Core

- Routes and forwards packets from source to destination.
- Handles congestion and optimizes resource utilization.
- Ensures reliability and scalability in data transmission.

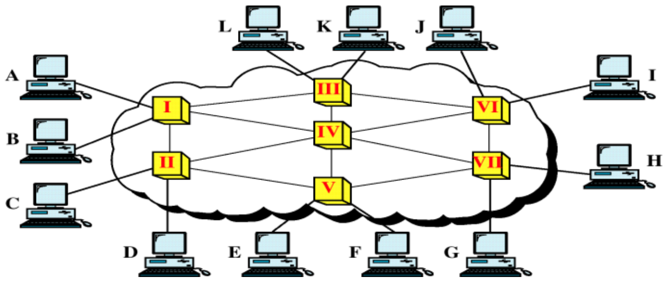
There are two fundamental methods used in the network core for data transfer:

1. Packet switching
2. Circuit switching

Introduction to Switching:

- A network is a set of connected devices.
- A switched network consists of a series of interlinked nodes, called switches.
- Switches are devices capable of creating temporary connections between two or more devices to the switch as shown in the figure.

Switched Network



- ➢ The end systems (communicating devices) are labeled A,B,C,D, and so on, and the switches are labeled I,II,III,IV,V,VI,VII.
- ➢ Each switch is connected to multiple links.

Packet switched Network (used in the Internet):

- ➢ In a packet-switched network, there is no resource reservation; resources are allocated on demand like first-cum first-served basis.
- ➢ Data is divided into small packets, which are transmitted independently across the network.
- ➢ Each packet contains header information, including the destination address.
- ➢ The routers decide the best route for each packet.

Characteristics of Packet Switching

- ➢ No dedicated path; packets can take different routes.
- ➢ More efficient than circuit switching because resources are shared dynamically.
- ➢ Supports multiple users without reserving bandwidth.

Advantages of Packet Switching

- ➢ Efficient resource utilization – Bandwidth is shared among many users.
- ➢ Scalability – Can support a large number of simultaneous connections.
- ➢ Fault tolerance – If a route fails, packets can be rerouted.

Disadvantages of Packet Switching

- ➢ Potential for congestion – Multiple users sharing the same link can lead to delays.
- ➢ Packets can arrive out of order – Since each packet can take a different path.
- ➢ Packet loss – If network congestion is too high, packets may be dropped.

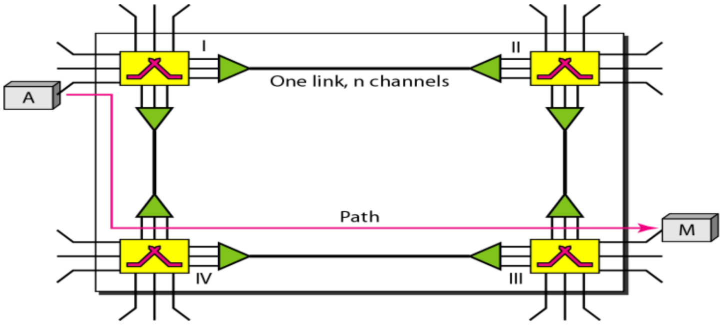
Store-and-Forward Transmission

In packet switching, routers follow a store-and-forward mechanism:

1. A router **receives the entire packet** before forwarding it.
2. If the **outgoing link** is busy, the packet is stored in a queue.
3. Once the link is free, the packet is **forwarded to the next router**.

Circuit-switched networks (used in Telephone networks):

- ➢ In circuit-switched networks, a dedicated communication path is established between sender and receiver before communication begins.
- ➢ Figure shows a trivial circuit-switched network with four switches and four links where each link is divided into n(n=3 in the figure) channels.



The actual communication in a circuit-switched network requires three phases:

1. Connection setup
2. Data transfer
3. Connection tear down

Connection setup:

A dedicated path is reserved.

Data Transfer Phase:

- ➢ After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase:

- ➢ When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Example of Circuit Switching

- Public Switched Telephone Network (PSTN)
- Integrated Services Digital Network (ISDN)

Advantages:

- Guaranteed bandwidth (suitable for voice and real-time applications).
- Fixed latency **(low delay once the connection is established).**

Disadvantages of Circuit Switching

- Inefficient for bursty data traffic – If a user isn't continuously sending data, reserved resources are wasted.
- Setup delay – Establishing a circuit before communication takes time.
- Scalability issues – Fixed circuits limit the number of simultaneous connections.

Delay, Loss, and Throughput in Packet-Switched Networks:

Introduction:

In packet-switched networks, packets travel through multiple routers and links before reaching their destination. Along the way, they may experience delay, loss, and throughput limitations, which affect the overall performance of network communication.

Delay in Packet-Switched Networks:

Delay refers to the time a packet takes to travel from the source to the destination. It consists of four key components:

Types of Delay

1. Processing Delay (D_{proc})
    - Time taken by a router/switch to process a packet before forwarding it.
    - Includes error checking, routing table lookup, and protocol processing.
    - Typically in the range of microseconds (µs).
2. Queuing Delay (D_{queue})
    - Time a packet waits in a router's queue before being transmitted.
    - Depends on network congestion and traffic load.
    - Can range from zero (no congestion) to several milliseconds (high congestion).

3. Transmission Delay (D_{trans})

   - Time required to push all bits of a packet onto the link.
   - Calculated as:

     $D_{trans} = L/R$

     Where:

     - L = Packet size (in bits)
     - R = Transmission rate (bits per second)

   - Example:

     If a 1,000-bit packet is transmitted over a 10 Mbps link:

     $D_{trans} = 1000/10^7 = 0.1\text{ ms} = 100\ \mu s$

4. Propagation Delay (D_{prop})

   - Time for a bit to physically travel from sender to receiver over a medium.
   - Calculated as:

     $D_{prop} = d/s$

     Where:

     - d = Distance (meters)
     - s = Propagation speed ($\approx 2\times10^8$ m/s for fiber optics)

   - Example:

     If a signal travels 10,000 km (10,000,000 m):

     $D_{prop} = 10{,}000{,}000 / 2 \times 10^8 = 50\text{ ms}$

End-to-End Delay Calculation

Total delay from source to destination:

$$D_{end\text{-}to\text{-}end} = D_{proc} + D_{queue} + D_{trans} + D_{prop}$$

For multiple routers, delays add up at each hop.

Packet Loss in Packet-Switched Networks:

Packet loss occurs when packets fail to reach their destination due to:

- Network congestion (router queues overflow).
- Bit errors (corrupted packets).
- Routing errors (packets dropped due to misconfiguration).

Causes of Packet Loss

- If a router's buffer (queue) is full, incoming packets are dropped (lost).
- TCP detects loss and retransmits missing packets, but this increases delay.
- UDP does not retransmit, leading to data loss in real-time applications (VoIP, video streaming).

Impact of Packet Loss

- TCP: Retransmits lost packets, leading to higher delay and reduced throughput.
- UDP: No retransmissions, leading to glitches, buffering, or missing data.

Throughput in Packet-Switched Networks:

Throughput measures the rate at which data is successfully transmitted over a network.

Types of Throughput

1. Instantaneous Throughput
   - The rate at a given instant.
   - Changes with network conditions.
2. Average Throughput
   - The total data transmitted divided by the total time taken.
   - Given by:

Average Throughput = Total data sent / Total time taken

Factors Affecting Throughput

- Network bandwidth: Higher bandwidth means higher potential throughput.
- Network congestion: More traffic reduces available throughput.
- Packet loss & retransmissions: Reduce effective throughput (TCP overhead).

Bottleneck Link in Throughput

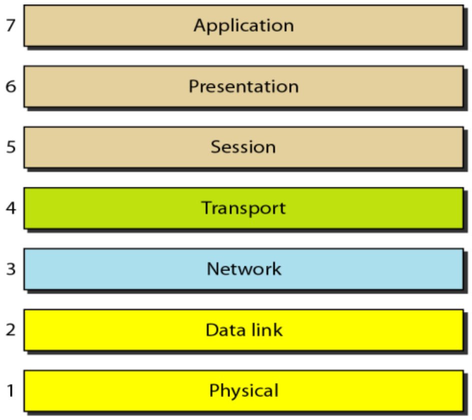
- The link with the lowest transmission rate determines the end-to-end throughput.
- Example: If a path has multiple links:
  - R1 = 10 Mbps
  - R2 = 5 Mbps
  - R3 = 1 Mbps
- The bottleneck is 1 Mbps, so total throughput cannot exceed 1 Mbps.

Network Models:

- A network is a combination of hardware and software that sends data from one location to another.
- There are two popular reference models. They are OSI (Open Systems Interconnection), TCP/IP (Transmission Control Protocol/Internet Protocol).

OSI Layered Architecture:

- It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network as shown in the figure.



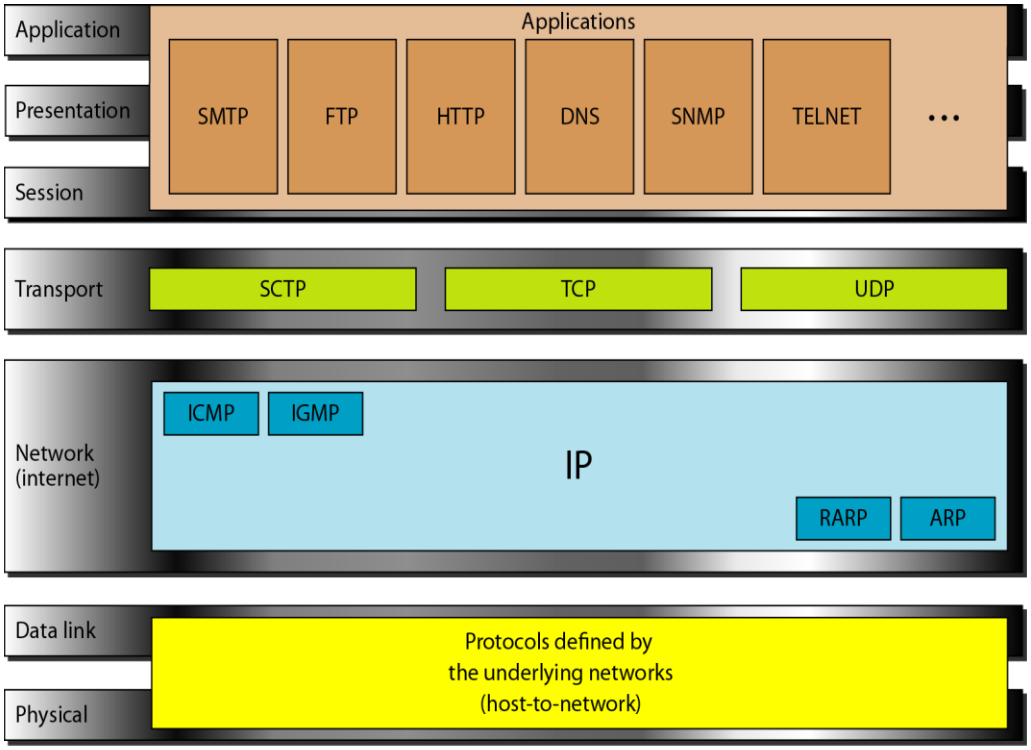
- The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

Summary of layers:

Layer	Function	Example Protocols
7. Application	Provides network services to applications	HTTP, FTP, SMTP, DNS
6. Presentation	Data translation, encryption, compression	SSL/TLS, JPEG, MPEG
5. Session	Manages communication sessions	NetBIOS, RPC
4. Transport	Reliable data transfer, flow control	TCP, UDP
3. Network	Routing and addressing	IP, ICMP, RIP
2. Data Link	Error detection, MAC addressing	Ethernet, Wi-Fi, PPP
1. Physical	Transmission of bits over a medium	Fiber, Copper, Radio Waves

TCP/IP Protocol Suite

- When TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.



Physical and Data Link Layers:

- At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCP/IP internet work can be a local-area network or a wide-area network.

Network Layer:

- At the network layer, TCP/IP supports the Internetworking Protocol (IP) and uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

IP:

- IP transports data in packets called datagrams, each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
- IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

Reverse Address Resolution Protocol (RARP):

- The Reverse Address Resolution Protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.
- It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

Internet Control Message Protocol(ICMP):

- The Internet Control Message Protocol (ICMP) is a mechanism which sends query and error reporting messages.

Internet Group Message Protocol (IGMP):

- The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer:

- Traditionally the transport layer was represented in TCP/IPby two protocols: TCP and UDP. To meet the needs of some newer applications SCTP protocol is introduced.

User Datagram Protocol (UDP):

- It is a process-to-process (connection less) protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

Transmission Control Protocol (TCP):

- TCP is a reliable connection-oriented protocol.That is, a connection must be established between both endsof a transmission before either can transmit data.

Stream Control Transmission Protocol (SCTP):

- It provides support for newer applications such as voice over the Internet.

Application Layer:

- It is equivalent to the combined session, presentation, and application layers in the OSI model.

A Comparison ofthe OSI and TCP/IP Reference Models:

OSI	TCP/IP
Three concepts are central to the OSI model: 1. Services: It tells what the layer does and the layer's semantics. 2. Interfaces: It specifies what parameters are to be used and what results are to expect. 3. Protocols: To provide the offered services.	The TCP/IP model did not originally clearly distinguish between service, interface, and protocol.
The protocols in the OSI model are better hidden and can be replaced relatively easily as the technology changes.	The protocols in this model are not hidden properly and so it is difficult to replace them as the technology changes.
The OSI reference model was devised before the corresponding protocols were invented. So the designers did not have much experience with the subject and did not have a good idea of which functionality to put in which layer.	Here the protocols came first, and the model was really just a description of the existing protocols. There was no problem with the protocols fitting the model.
The OSI model has seven layers.	The TCP/IP has four layers.
The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication is preferred in the transport layer.	The TCP/IP model has only one model in the network layer (connectionless) but supports both modes in the transport layer, giving the user a choice. This choice is especially important for simple request-response protocols.

Protocol Layers and their Service Models:

Introduction to Service Models:

A **service model** defines the type of **communication service** a network provides to applications. Different layers of a network stack offer **various service models**, ensuring that data is transmitted efficiently, reliably, and securely.

Types of Service Models

Service models can be classified based on how they manage **connections, reliability, and guarantees**.

Connection-Oriented vs. Connectionless Services

Service Type	Definition	Example Protocols
Connection-Oriented	Establishes a dedicated connection before communication	TCP
Connectionless	Sends data without a pre-established connection	UDP

- TCP (Transmission Control Protocol) **creates a** virtual connection **between sender and receiver before exchanging data.**
- UDP (User Datagram Protocol) **sends packets** independently**, without establishing a connection.**

Reliable vs. Unreliable Services

Service Type	Definition	Example Protocols
Reliable	Ensures data arrives correctly and in order	TCP
Unreliable	No guarantees on delivery or order	UDP

- Reliable services provide error detection, retransmission, and flow control.
- Unreliable services are faster but may result in packet loss or reordering.

Best-Effort vs. Guaranteed Services

Service Type	Definition	Example Protocols
Best-Effort Service	The network tries to deliver packets but makes no guarantees	IP
Guaranteed Service	Ensures specific delivery parameters like delay and bandwidth	MPLS, QoS protocols

- Best-Effort Service (Internet Model): The Internet follows a best-effort approach, meaning that packets may be lost, delayed, or arrive out of order.
- Guaranteed Service is used in specialized networks, such as real-time applications and private enterprise networks, where Quality of Service (QoS) techniques ensure bandwidth and low delay.

*****