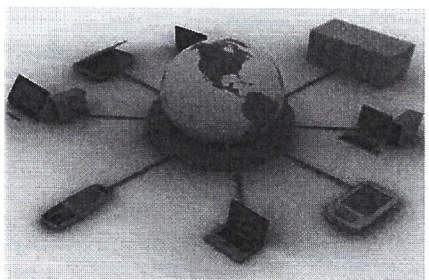
Web Technologies
23MX15
Reference material

23MX15 Web Technologies

- What is a Computer Network?
- A group of computing devise which are connected to each other and follow similar usage protocols for the purpose of sharing information and having communications provided by the networking nodes is called a Computer Network.

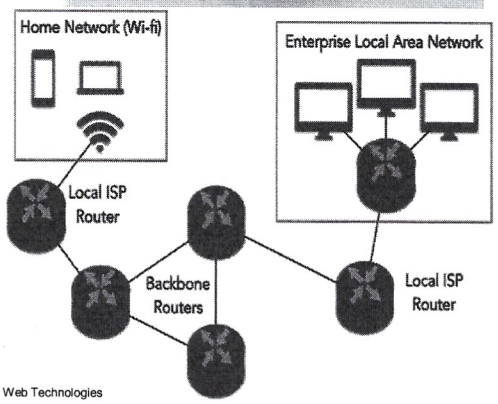


- Internetwork?

A collection of independent networks connected through interconnecting devices like routers.

- Internet?

The internet is a globally connected network system facilitating worldwide communication and access to data resources through a huge collection of personal, public, business, academic and government networks.



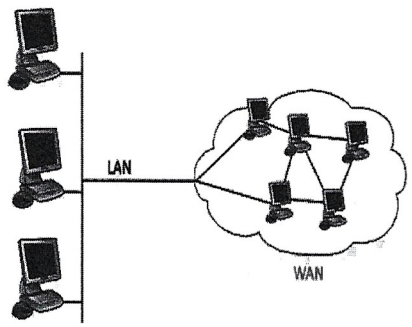
23MX15 Web Technologies

Types of Computer Networks

- Computer networks may be classified by many criteria, including the transmission medium (Guided or unguided media) used to carry signals, bandwidth (the maximum rate of data transfer across a given path), communications protocols to organize network traffic (the maximum rate of data transfer across a given path), the network size, the topology, traffic control (the process of managing, controlling or reducing the network traffic,) mechanisms, and organizational intent (VPN etc.,)

Types (size, coverage)

1. LAN - Local Area Network
2. MAN – Metropolitan Area Network
3. WAN – Wide Area Network
4. PAN – Personal Area Network
5. VPN – Virtual Private Network

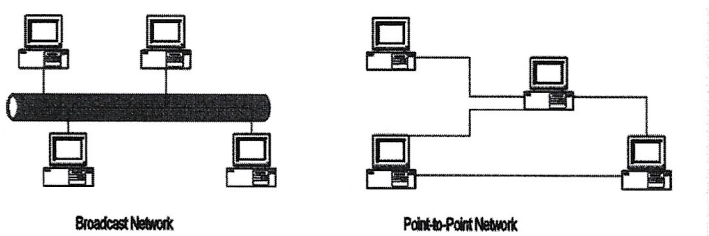


Internet vs WWW?

Two types of networks

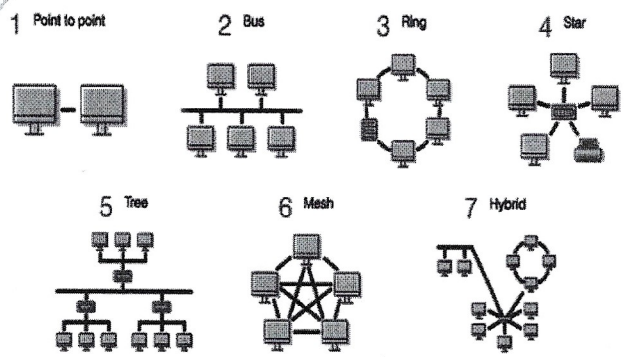
–Broadcast Networks: All stations share a single communication channel

–Point-to-Point Networks: Pairs of hosts (or routers) are directly connected



–Typically, local area networks (LANs) are broadcast and interconnection of Wide Area Networks (WANs) are point-to-point

Network Topology Types

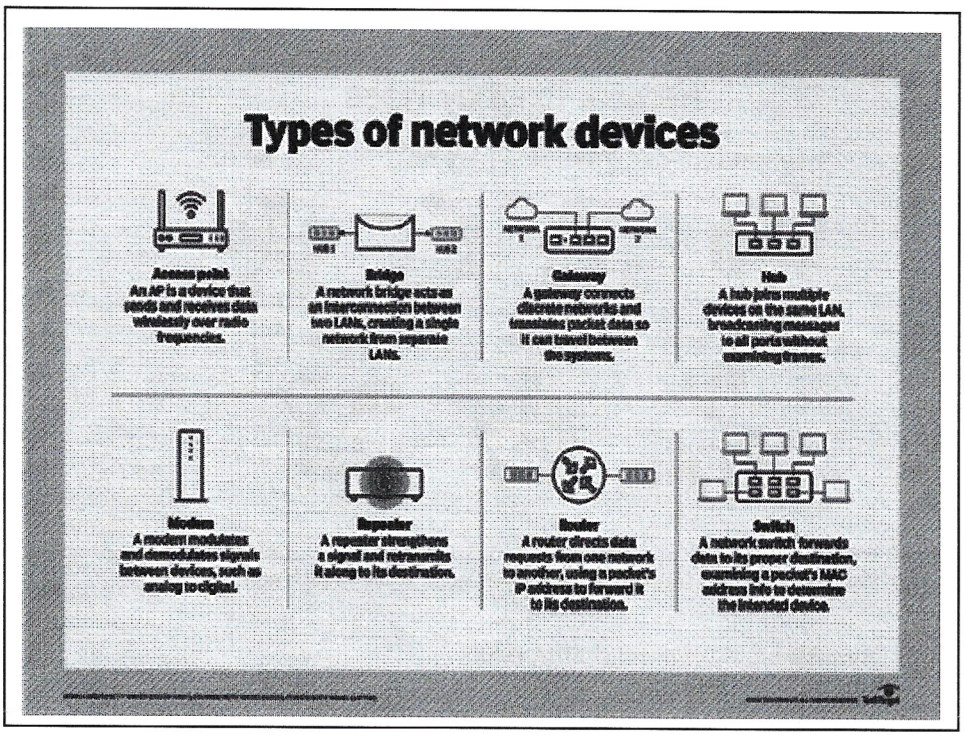


Network topology (geometrical) is the way a network is arranged, including the physical or logical description of how links and nodes are set up to relate to each other.

https://www.dnsstuff.com/what-is-network-topology

Network Topologies

- Given below are the eight types of Network Topologies:
- **Point to Point Topology** – Point to Point topology is the simplest topology that connects two nodes directly together with a common link.
- **Bus Topology** – A bus topology is such that there is a single line to which all nodes are connected and the nodes connect only to the bus
- **Mesh Topology** – This type of topology contains at least two nodes with two or more paths between them
- **Ring Topology** – In this topology every node has exactly two branches connected to it. If the ring is broken, or cannot work if one of the nodes on the ring fails
- **Star Topology** – In this network topology, the peripheral nodes are connected to a central node, which rebroadcasts all the transmissions received from any peripheral node to all peripheral nodes on the network, including the originating node
- **Tree Topology** – In this type of topology nodes are connected in the form of a tree. The function of the central node in this topology may be distributed
- **Hybrid Topology** – When two more types of topologies combine together, they form a Hybrid topology



Network Devices

- **Network Repeater** – Used to regenerate incoming electrical, wireless or optical signals
- **Network Hub** – It is a small network device. It joins multiple computers together to form a single network segment. On this segment, all computers can interact with each other
- **Network Switch** – It is a small hardware device which joins multiple computers together with a single LAN
- **Network Router** – This device interfaces in multiple networks whose task is to copy packages from one network to another. It provides connectivity inside enterprises, between Enterprises and the Internet and within an ISP
- **Network Bridge** – It reads the outermost section of the data packet to tell where the message is going. It reduces the traffic on other network segments.
- **Modem** – This device converts digital signals into analog signals. It is always placed between a telephone and a computer system.

https://blog.netwrix.com/2019/01/08/network-devices-explained/

Layered Architecture of ISO/OSI

- OSI Reference Model - internationally standardised network architecture.
- OSI = *Open Systems Interconnection*: deals with *open systems*, i.e. systems open for communications with other systems.
- Specified in ISO 7498.
- Model has 7 layers.

The grouping of relevant communication functions into different hierarchical sets is known as layering.
It involves
Service: A collection of functions provided by a layer to a higher layer.
Protocol: A set of rules to share data with the peer layer.
Interface: This is a means of transmitting a message from one layer to another.

Each layer is responsible for the following functions:

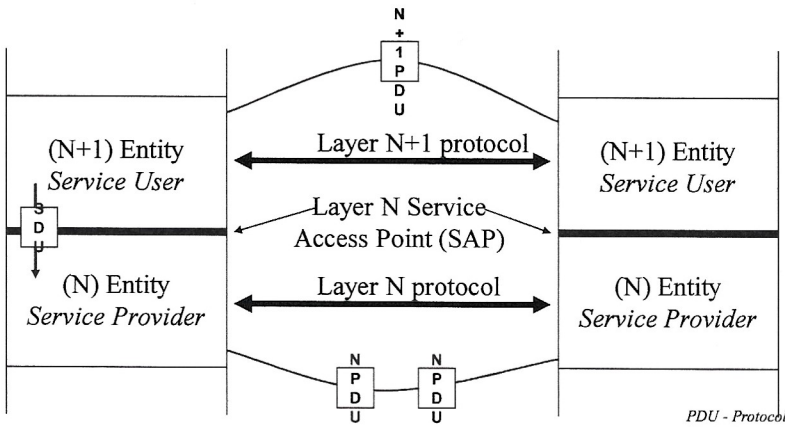
- Perform a subset of different functions required for communication.
- Provide the services of its functions to the next higher layer in the hierarchy.
- Implementation of communication protocols with peer layers in another system.
- After implementing its operations, it relies on the next layer to perform additional functions.
- When two computers communicate on a network, the software at each layer on one computer assumes it is communicating with the same layer on the other computer.

Advantages of Layered Architecture of Computer Networking

- Reduces complexity - It breaks network communication into smaller, simpler parts. It divides the network communication process into smaller and simpler components, thus aiding component development, design, and troubleshooting.
- Standardizes interfaces - It standardizes network components to allow multiple vendor development and support.
- Facilitates modular engineering - It allows different types of network hardware and software to communicate with each other.
- Interoperability between Vendors - It allows multiple-vendor development through standardization of network components. Defines the process for connecting two layers together and eases troubleshooting and implementation.
- Ensures interoperable technology - It prevents changes in one layer from affecting the other layers, allowing for quicker development.
- Accelerates evolution - It provides for effective updates and improvements to individual components without affecting other components or having to rewrite the entire protocol.

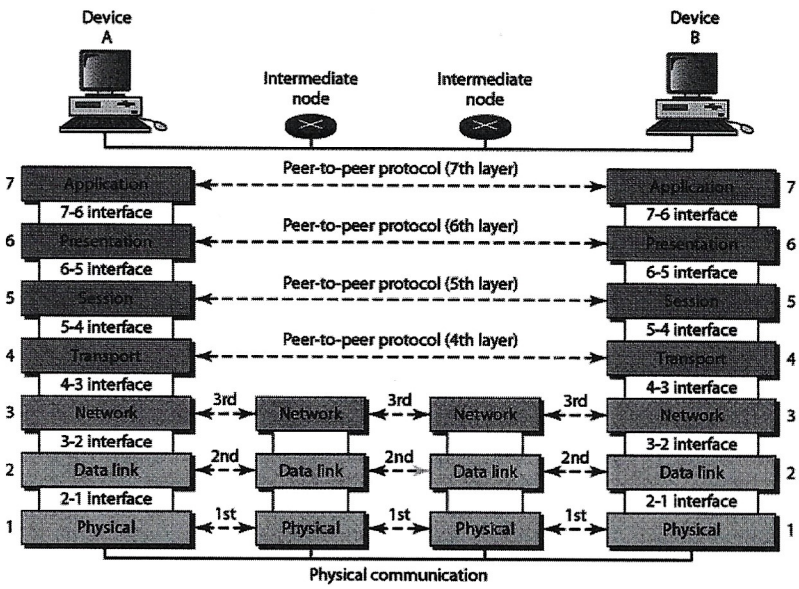
The process of encapsulating data layer by layer enables the services at the different layers to develop and scale without affecting other layers

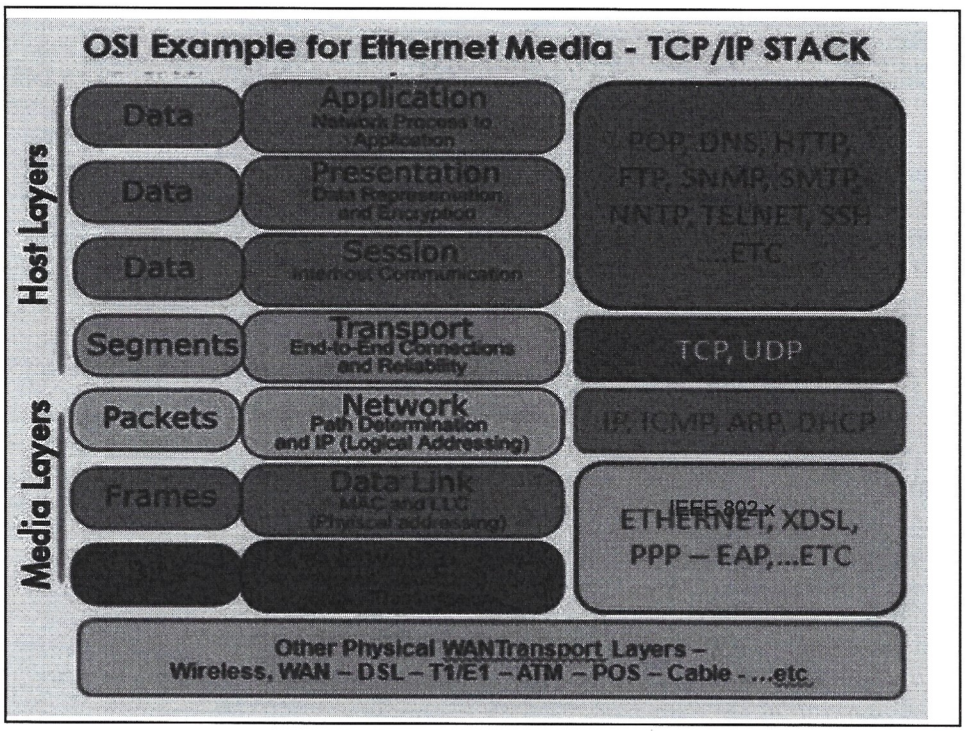
Layering Principles



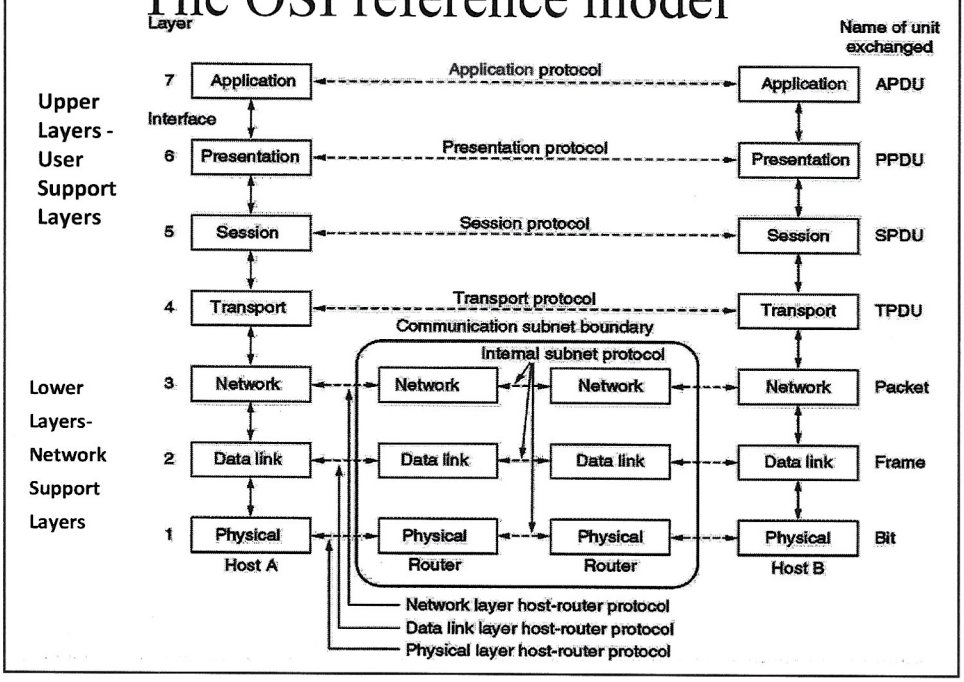
- Layer N provides service to layer N+1

The interaction between layers in the OSI model



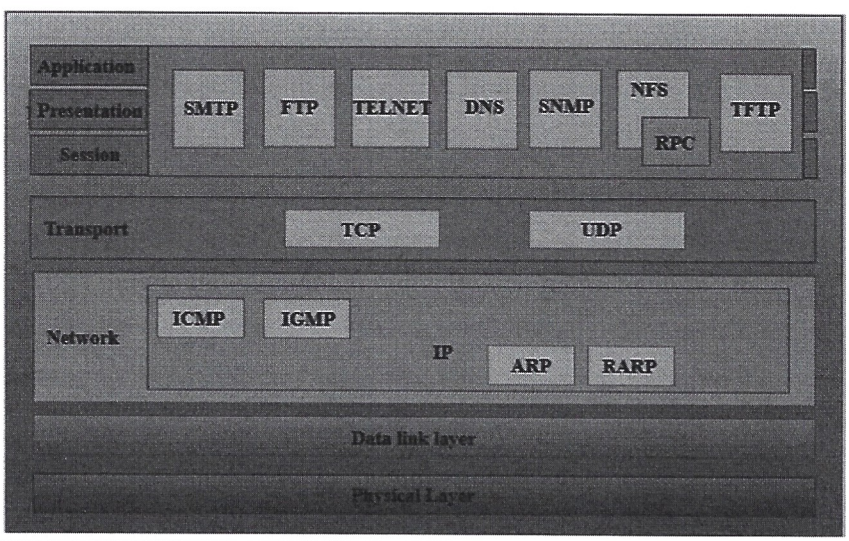


The OSI reference model



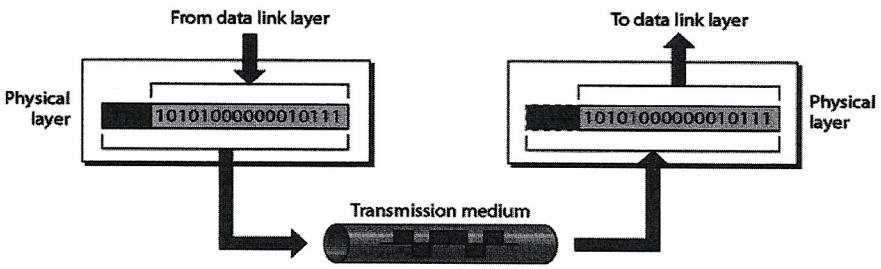
TCP/IP Layered architecture

TCP/IP Protocol stack



Physical layer - **Physically carries the information from one end of the link to the other end.**

The physical layer is responsible for movements of individual bits from one node to the next.

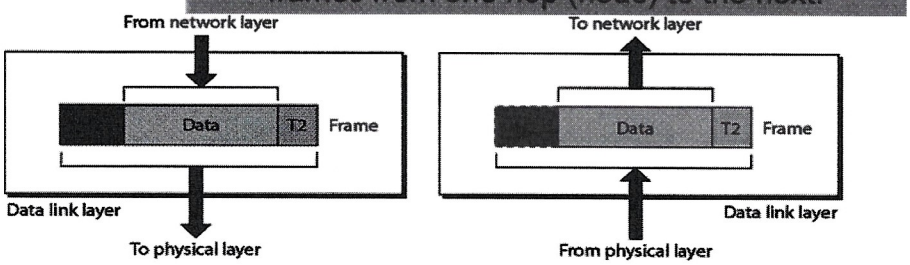


Functions :

1. Defining the physical characteristics of interfaces and medium and also its types
2. Representation of bits as signals and vice versa– using encoding and decoding techniques
3. Defining the duration time of a bit.
4. Synchronizing the sender and the receiver clocks.
5. Connecting devices to the medium in point-to-point or multipoint configuration.
6. Defining how devices are geometrically connected to make a network.
7. Defining the direction of transmission between two devices.

Data link layer

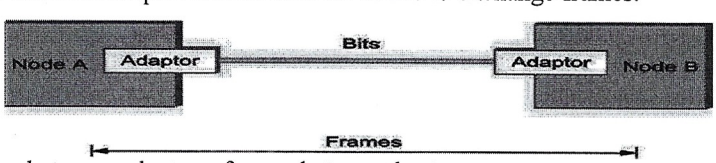
The data link layer is responsible for moving frames from one hop (node) to the next.



Framing

The focus is on packet-switched networks, which means that blocks of data (called *frames* at this level), not bit streams, are exchanged between nodes.

It is the network adaptor that enables the nodes to exchange frames.



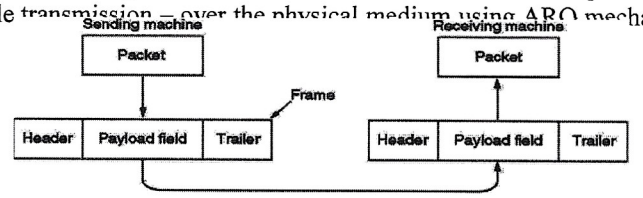
Bits flow between adaptors, frames between hosts

Data Link Layer

- **provides reliable communication over the unreliable physical link**

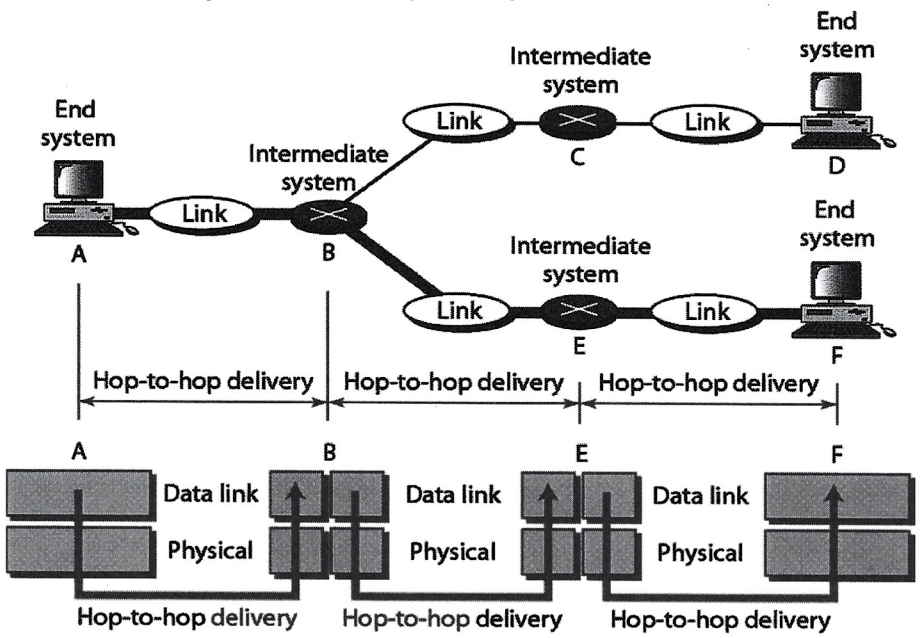
Functions

- Framing – Breaks the outgoing data into frames and reassemble the incoming bits.
- Line Discipline – Manages the start of the communication
- Flow Control – How many frames to send without overwhelming the receiver.
- Error Control – Handles error by implementing Acknowledgement and retransmission schemes.
- Access Control – Manages the broadcast links
- Physical addressing - attaches the MAC address in the header part and a trailer.
- Reliable transmission – over the physical medium using ARQ mechanism.



Piggybacking is a process of attaching acknowledgment with the data packet to be sent. It is used to improve the efficiency of the bidirectional protocols.

Data Link Layer - *Hop-to-hop delivery*



Network Layer - host to host

Functions:

Routing: It routes the signal through different channels from one network . It acts as a network controller. It manages the subnet traffic. It decides by which route data should be transmitted.

Packetizing: It divides the outgoing messages into manageable packets.

Logical Addressing: Attaches logical address of source and destination machines.

Address Resolution: It determines the physical address of the next hop.

Devices: Routers and gateways operate in the network layer.

Route determination: Best route is chosen for routing the packets to final destination. (uses routing algorithms)

Switching: Move packets from router's input to appropriate router output. Uses packet switching or virtual circuit switching.

Network Layer Functions - contd..

Error Control: Header part of the IP datagram is validated at each router using checksum.

Flow Control: No flow control service in NW layer. Why? The flow control is provided for most of the upper layer protocols that use the services of the network layer, so another level of flow control makes the network layer more complicated and the whole system less proficient.

Congestion Control: Congestion in a connectionless network can also be implemented using a choke packet, a special packet that can be sent from a router to the sender when it encounters congestion. This mechanism, is implemented in the Internet network layer. The network layer uses an auxiliary protocol, ICMP . When a router is congested, it can send an ICMP packet to the source to slow down.

Security : No security in Network Layer? The network layer was designed with no security provision.

Today, however, security is a big concern. To provide security for a connectionless network layer, we need to have another virtual level that changes the connectionless service to a connection-oriented service. This virtual layer is called **IPSec** which is implemented as optional one in latest TCP/IP .

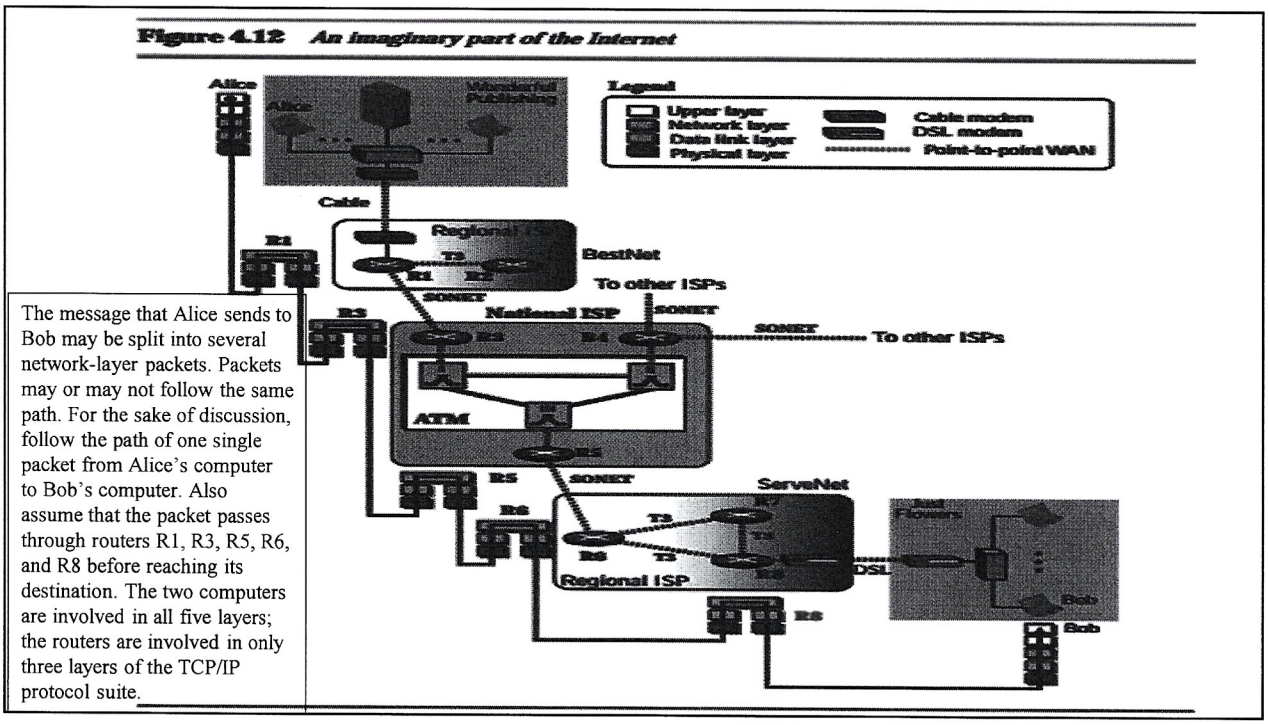
Network Layer

The network layer at the source computer provides four services: packetizing, finding the logical address of the next hop, finding the physical (MAC) address of the next hop, and fragmenting the datagram if necessary.

The network layer receives several pieces of information from the upper layer:

Data, length of data, logical destination address, protocol ID (mainly TCP or UDP , the identifier of the protocol using the network layer), and service type .

The network layer processes these pieces of information to create a set of fragmented datagrams and the next-hop MAC address and delivered them to the data link layer.



The message that Alice sends to Bob may be split into several network-layer packets. Packets may or may not follow the same path. For the sake of discussion, follow the path of one single packet from Alice's computer to Bob's computer. Also assume that the packet passes through routers R1, R3, R5, R6, and R8 before reaching its destination. The two computers are involved in all five layers; the routers are involved in only three layers of the TCP/IP protocol suite.

Transport Layer - end-to-end delivery

- Provides efficient, reliable, cost-effective service to processes in Application Layer using the services provided by the unreliable Network Layer.
- Provides a service on top of the unreliable network.
- It provides a logical connection between two hosts.

The main functions of this layer are the following: -

- **Segmentation and Addressing** : Attaches port address (16 bit) to each of the segments formed. Local process and remote process are identified using port numbers. Many of these are defined by ICANN.
- **Reliable Service:** Through error and flow control.
- **Data Integrity and Error detection (control)** :: Using checksum and ACK & NACK packets
- Flow control - TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It is achieved through sliding window protocol.

Transport Layer - end-to-end delivery

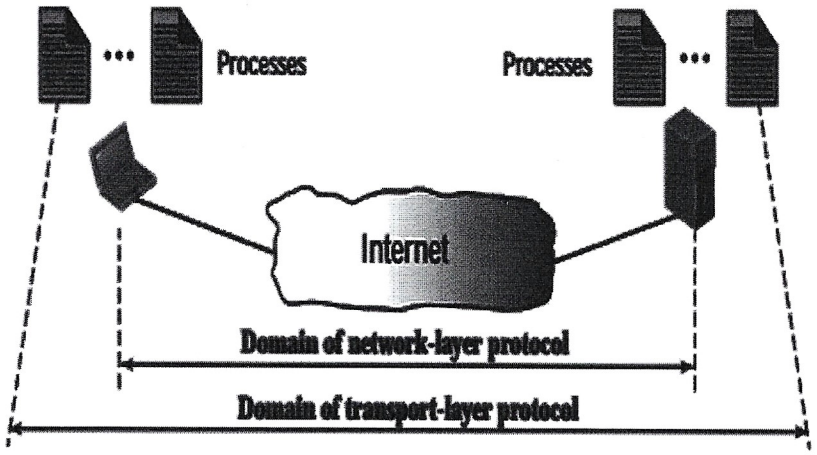
Functions - contd...

- **Connection multiplexing :** The transport layer at the source performs multiplexing; the transport layer at the destination performs demultiplexing. Transport layer receives the segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.
- **Congestion Control:** It uses **open loop** congestion control to prevent the congestion and **closed-loop** congestion control to remove the congestion in a network once it occurred. TCP provides AIMD- additive increase multiplicative decrease, leaky bucket technique for congestion control.
- **Encapsulation and Decapsulation :**

When a process has a message to send, it passes the message to the transport layer along with a pair of socket addresses and some other pieces of information that depends on the transport layer protocol. The transport layer receives the data and encapsulate these as transport-layer header.

- Decapsulation happens at the receiver site. When the message arrives at the destination transport layer, the header is dropped and the transport layer delivers the message to the process running at the application layer. The sender socket address is passed to the process in case it needs to respond to the message received.

Figure 13.1 *Network layer versus transport layer*



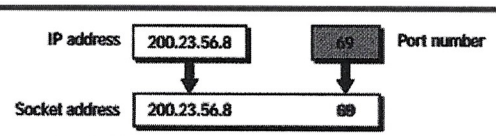
Socket Addressing

A transport-layer protocol in the TCP suite needs both the IP address and the port number(16 bits) , at each end, to make a connection. ***The combination of an IP address and a port number is called a socket address.***

The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely. To use the services of transport layer in the Internet, a pair of socket addresses : the client socket address and the server socket address is needed.

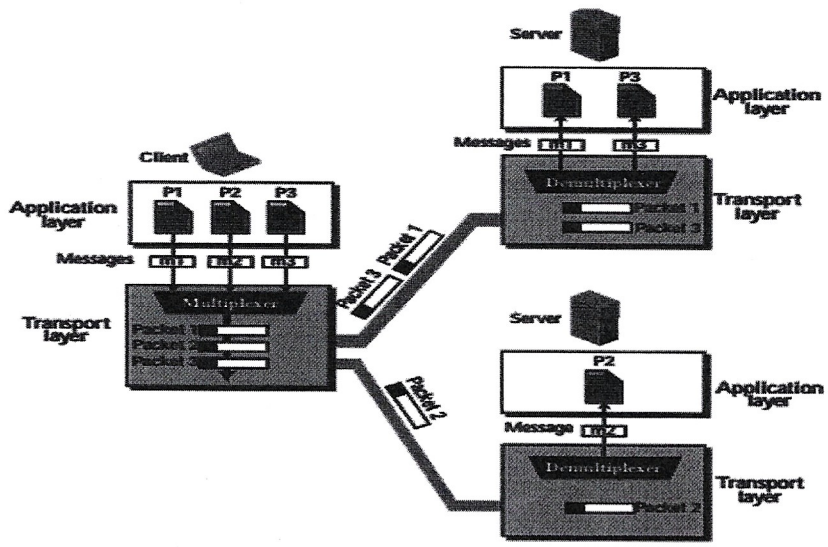
These four pieces (client and server IP, client and server port address) of information are part of the network-layer packet header and the transport-layer packet header. The first header contains the IP addresses; the second header contains the port numbers.

Figure 13.5 *Socket address*



Transport layer receives the segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.

Figure 13.7 ***Multiplexing and demultiplexing***



Reliable Stream Transport Service

Why at Transport layer ???

ØLower layers deliver packets out of order, with substantial delay, deliver duplicates where in packets can be lost or destroyed.

ØApplication programs need to provide error detection and recovery into each application program.

ØImplementing a single general purpose solutions to the problems of providing reliable stream delivery for all application programs to use.

ØIsolate application programs from the details of networking, and makes it possible to define a uniform interface for the stream transfer service.

Transmission Control Protocol

Reliability

- Reliable services never lose/corrupt data.
- Reliable service costs more.
- Typical application for reliable service is file transfer.
- Typical application not needing reliable service is voice traffic.
- Not all applications need connections.

•Reliable stream transport

•Connection oriented (full duplex virtual circuit) - ike telephone system.

–Conceptually place call, two ends communicate to agree on details

–After agreeing application notified of connection

–During transfer, ends communicate continuously to verify data received correctly

–When done, ends tear down the connection

–If UDP is like regular mail, TCP is like phone call

•Provides buffering and flow control

•Takes care of lost packets, out of order, duplicates, long delays – by Positive ACK Retransmission mechanism

•Isolates application program from network Hardware details

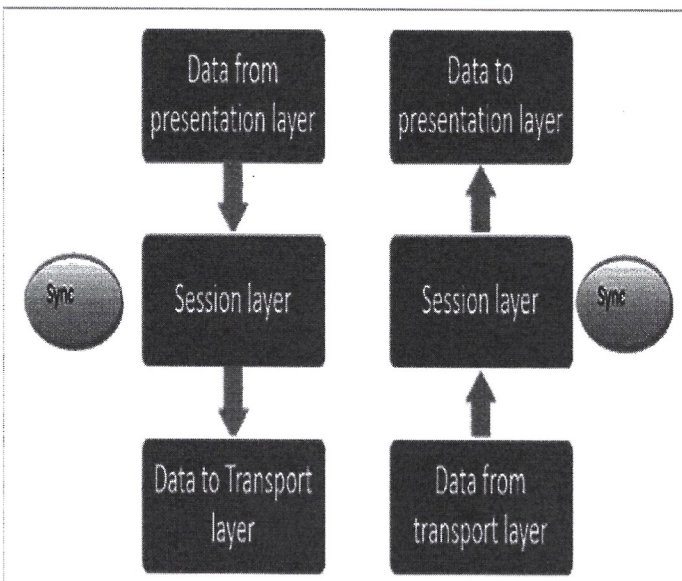
•Jargon

–Segment = TCP packet

–Socket= source (address + port) + destination (address + port)

Session Layer

- Permits the users of different platforms to set up an active communication session between themselves.
- Provides synchronization between distinctive applications. The synchronization is necessary for efficient delivery of data without any loss at the receiver end.
- Place different checkpoints while sending a large file.



16

Presentation Layer

- Present the data to its end users in the form in which it can easily be understood.
- It plays the role of a translator so that the two systems come on the same platform for communication and will easily understand each other.
- The data which is in the form of characters and numbers are split into bits before transmission by the layer. It translates the data for networks in the form in which they require it and for devices like phones, PC, etc in the format they require it.
- Does encryption and Decryption
- Does compression and decompression for efficient use of bandwidth on large files.

17

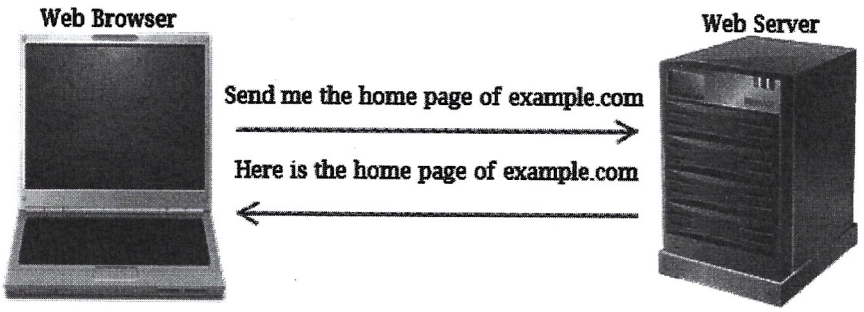
Application Layer

- This is the topmost and seventh layer of the OSI reference model. This layer will communicate with the operating system, with the end users & user applications
- This layer grants a direct interface and access to the users with the network. The users can directly access the network at this layer. Few **Examples** of services provided by this layer include e-mail, sharing data files, FTP GUI based softwares , remote login (used for file access) , telnet network devices etc.
- It enables authentication between devices for an extra layer of network security.
- It also checks whether the sender's computer has the necessary communication interfaces, such as an Ethernet or Wi-Fi interface. The data on the receiving end is presented to the user application.

- AL protocols : DNS, DHCP, FTP, TELNET, SMTP, HTTP, SNMP etc.,

18

At Application Layer



The HTTP protocol manages the communication between the web browser and the webserver. It is a language that web browsers and web servers understand and use to provide the necessary information.

When we type a URL in the address bar of a web browser and press the Enter key, the HTTP protocol finds the destination address, gets the requested content from the destination host, and displays the received content. If the requested content is not available, it displays an error message.

The Application layer does not define any application. It only defines the standards, services, and protocols that an application needs to connect to a remote computer. HTTP, HTTPS, SNMP, NTP, SSH, FTP, TFTP, Telnet, DHCP, and DNS are examples of application layer protocols.

19

(Not for Exam)

Internet Assigned Numbers Authority (IANA) and Internet Corporation for Assigned Names and Numbers (ICANN)

The Internet Assigned Numbers Authority (IANA), supported by the U.S. government, was responsible for the management of Internet domain names and addresses until October 1998.

After that the Internet Corporation for Assigned Names and Numbers (ICANN), a private nonprofit corporation managed by an international board, assumed IANA operations

Other Controlling coporations are, IAB, IETF, ISOC, IRTF etc.,

Inventor of Internet?

BOB KAHN (1938–) AND VINT CERF (1943–)

American computer scientists who developed TCP/IP, the set of protocols that governs how data moves through a network. This helped the ARPANET evolve into the internet we use today. Vint Cerf is credited with the first written use of the word 'internet'.

For further information refer:

ietf.org The site of IETF

w3c.org The site of W3C standard organization

20