(*) Introduction

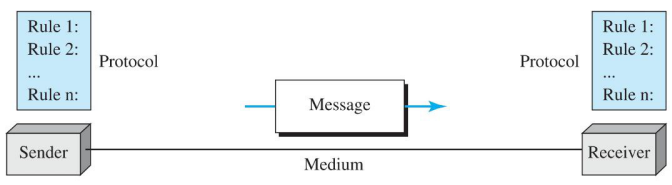
^ The largest computer network, the INTERNET, has billions of users in the world who use WIRED and WIRELESS transmission media to connect small and large computers.

DATA refers to INFORMATION presented in whatever FORM is agreed upon by the parties CREATING and USING it.
DATA COMMUNICATIONS is the exchange of DATA between two devices via a combination of HARDWARE (physical equipment) and SOFTWARE (programs).

The EFFECTIVENESS of a data communications system depends upon :-

1. DELIVERY –
   Delivery must be ensured ONLY to the CORRECT destination.
2. ACCURACY –
   Data ALTERED during transmission must be CORRECTED.
3. TIMELINESS –
   Data must be delivered AS they are produced, in the same ORDER that they are produced, and without significant DELAY.
4. JITTER –
   The variation in the ARRIVAL RATE of data must be minimized.

^ **Figure 1.1** *Five components of a data communications system*

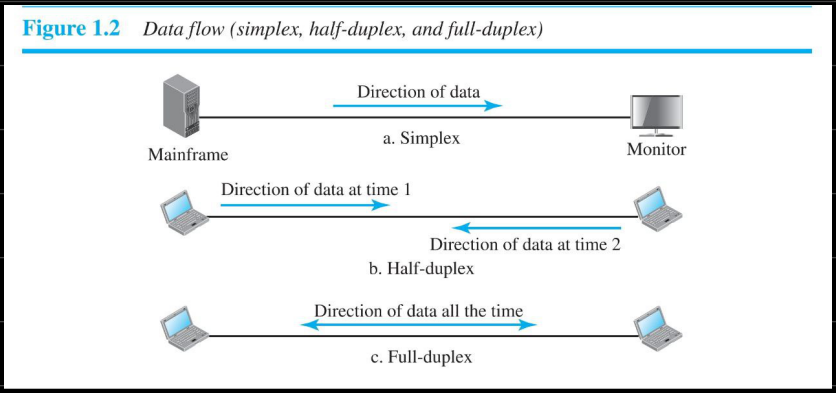


A protocol is a set of RULES.
Message is the DATA to be sent.
Medium can be CABLES, RADIO WAVES, etc.

Without a PROTOCOL, two devices may be CONNECTED but not able to COMMUNICATE, just as a person speaking French cannot be understood by a person who only speaks Japanese.

Data/Information can come in different FORMS, such as text, numbers, images, audio and video.

^



1. SIMPLEX –

   The communication is UNIDIRECTIONAL. Only one of the two devices on a link can TRANSMIT; the other can only RECEIVE. For eg., keyboards and traditional monitors.

2. HALF–DUPLEX –

   Each station can both TRANSMIT and RECEIVE, but NOT at the same time. For eg., walkie–talkies.

3. FULL–DUPLEX –

   Both stations can TRANSMIT and RECEIVE SIMULTANEOUSLY. For eg., telephone network.

^

A NETWORK is the interconnection of a set of DEVICES capable of COMMUNICATION, where a device can be a HOST (for eg., desktop) or a CONNECTING DEVICE (for eg., router).

Network criteria :–

1. PERFORMANCE –

   For eg., TRANSIT TIME (amount of time required for a MESSAGE to travel from one DEVICE to another), RESPONSE TIME (elapsed time between an INQUIRY and a RESPONSE), etc.

   These depend upon a number of FACTORS, for eg., the number of USERS, the TYPE of TRANSMISSION MEDIUM, etc.

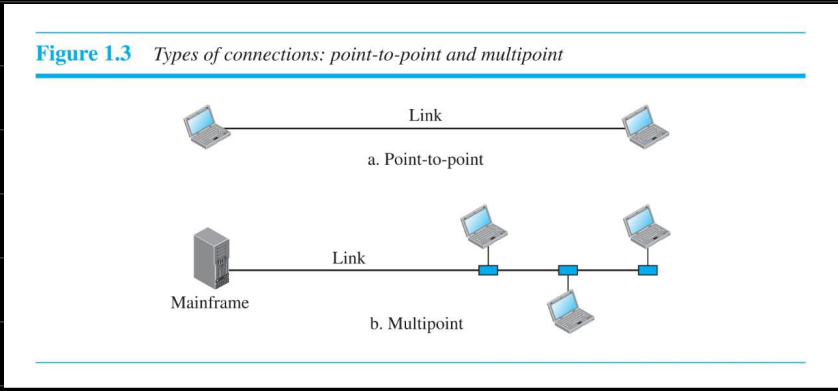
2. RELIABILITY –

   For eg., the frequency of FAILURE, RECOVERY time, etc.

3. SECURITY –

   For eg., protection from UNAUTHORIZED access, protection from DAMAGE, policies for recovery from BREACHES, etc.

^ In a network, devices are connected through LINKS. A link (also known as a CHANNEL) is a COMMUNICATION pathway that TRANSFERS data from one DEVICE to another. For communication to occur, two devices must be connected in some way to the SAME LINK at the SAME TIME.



1. POINT-TO-POINT CONNECTION –

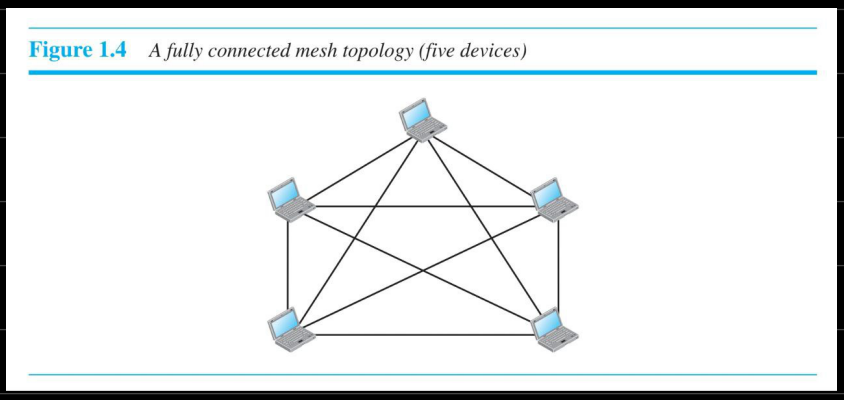
   It provides a DEDICATED link between TWO devices, and the ENTIRE capacity of the link is reserved for TRANSMISSION between those two devices ONLY.

2. MULTIPOINT/MULTIDROP CONNECTION –

   MORE than two devices share a single link, and the capacity of the link is shared, either SPATIALLY (i.e. if several devices can use the link SIMULTANEOUSLY) or TEMPORALLY (i.e. if the devices must take TURNS to use the link).

^ PHYSICAL TOPOLOGY refers to the way in which a network is laid out PHYSICALLY, i.e. it is the GEOMETRIC representation of the relationship of all the LINKS and the LINKING DEVICES (NODES) to one another.

1. MESH Topology –

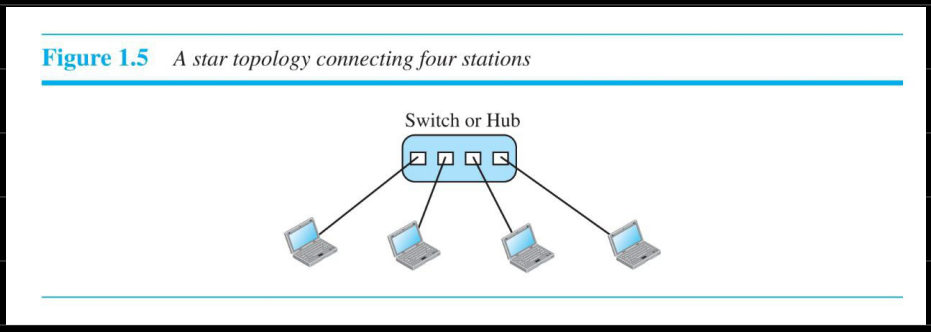


Every device has a dedicated POINT–TO–POINT link to every other device.

Total number of physical DUPLEX links = ${}^{n}C_{2}$ = n (n – 1) / 2, where n is the number of devices.

Every device must have n – 1 input/output (I/O) ports.

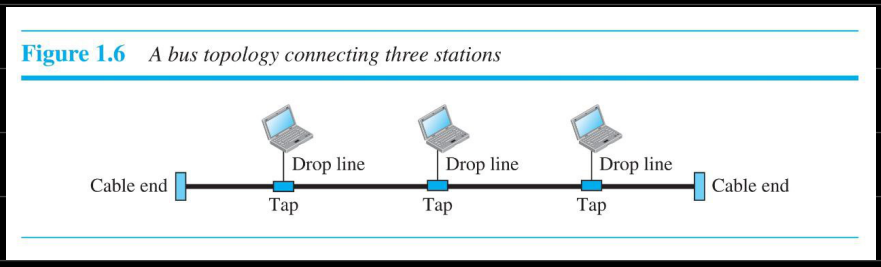
2. STAR Topology –



Each device has a dedicated POINT–TO–POINT link only to a CENTRAL controller, usually a HUB, and is NOT directly linked to any other device.

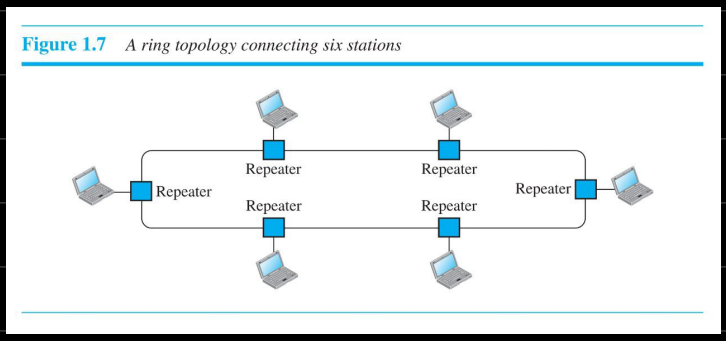
The controller acts as an EXCHANGE, i.e. if one device wants to send data to another, it sends the data to the CONTROLLER, which then relays the data to the target device.

3. BUS Topology –



Each device is connected to a MULTIPOINT link, which acts as a BACKBONE to link all the devices in the network. A DROP LINE is a connection running between the DEVICE and the MAIN CABLE. A TAP is a connector.

4. RING Topology –



Each device has a dedicated POINT-TO-POINT connection with only the TWO devices on either side of it. Data are passed along the ring in ONE direction, from device to device, until they reach the DESTINATION.

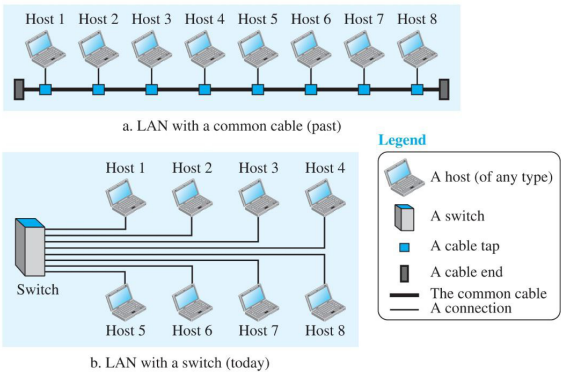
A REPEATER regenerates the BITS and passes them along.

^ Network Types :–

1. LOCAL AREA Network –

A LAN is usually PRIVATELY owned and connects SOME hosts in a single office, building or campus.

Figure 1.8 *An isolated LAN in the past and today*



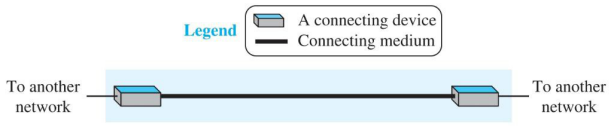
2. WIDE AREA Network –

A WAN has a WIDER geographical span than a LAN, spanning a town, a state, a country, or even the world.

A LAN interconnects HOSTS, whereas a WAN interconnects CONNECTING DEVICES, such as switches, routers or modems.

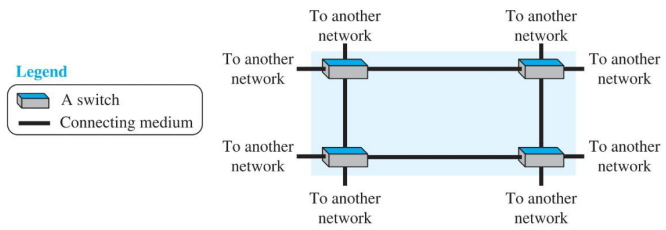
A POINT-TO-POINT WAN is a network that connects TWO communicating devices through a transmission medium.

Figure 1.9 *A point-to-point WAN*



A SWITCHED WAN is a network with MORE than two ends. It is used in the BACKBONE of a global communications network today.

Figure 1.10 *A switched WAN*



Most commonly, LANs and WANs are connected to one another, making an INTERNETWORK, i.e. an internet (lowercase i).

Figure 1.11 *An internetwork made of two LANs and one point-to-point WAN*

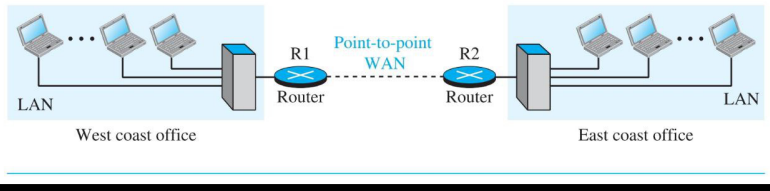
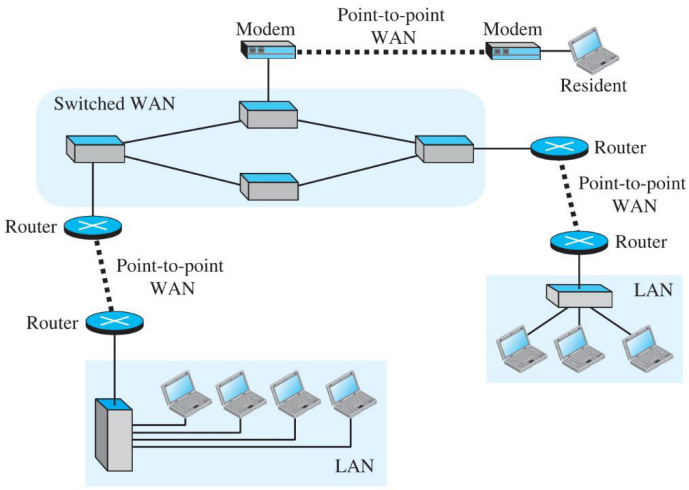
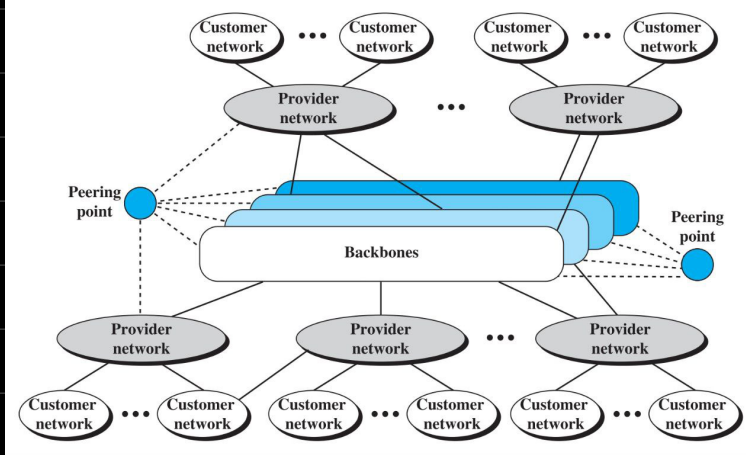


Figure 1.12 *A heterogeneous internetwork made of four WANs and two LANs*



The most notable internet is called the Internet (uppercase I) and is composed of THOUSANDS of interconnected networks.

Figure 1.13 *The Internet today*



At the top level, the BACKBONES (also known as INTERNATIONAL INTERNET SERVICE PROVIDERS (ISPs)) are large networks owned by some COMMUNICATION companies which are connected through complex SWITCHING systems, called PEERING points.

At the second level, there are smaller networks, called PROVIDER networks (also known as NATIONAL/REGIONAL ISPs), that use the services of the backbones for some FEES.

The CUSTOMER networks are networks at the edge of the Internet that actually use the services provided by the Internet by paying some FEES to provider networks.

^ Accessing the Internet

A physical connection to an ISP is done through a POINT-TO-POINT WAN. For eg.,

1. By using a TELEPHONE network, i.e. by changing the VOICE line to a point-to-point WAN through a DIAL-UP service (i.e. by using a MODEM to convert DATA to AUDIO SIGNALS and imitating making a telephone connection, thereby making the line UNUSABLE for normal telephone connections), or through a DSL (DIGITAL SUBSCRIBER LINE) service (i.e. the upgraded version of a dial-up service where the line can be used SIMULTANEOUSLY for voice and data communications).
2. By using a CABLE television network.
3. By using a WIRELESS network.
4. By DIRECTLY connecting to the Internet, for eg., by becoming a local ISP.

^ Protocol Layering

A PROTOCOL defines the RULES that the SENDER, the RECEIVER and all INTERMEDIATE devices need to follow to communicate effectively.

When communication is COMPLEX, we may need to divide the task of communicating among different LAYERS.

1. A SINGLE-layer protocol (2 friends talking to each other DIRECTLY) :-

Few examples of rules -

a. Greet the other person upon meeting.

b. Use proper words.

c. Don't speak when the other person is speaking.

d. Let the other person speak after you.

e. Bid farewell to the other person after the conversation is over.

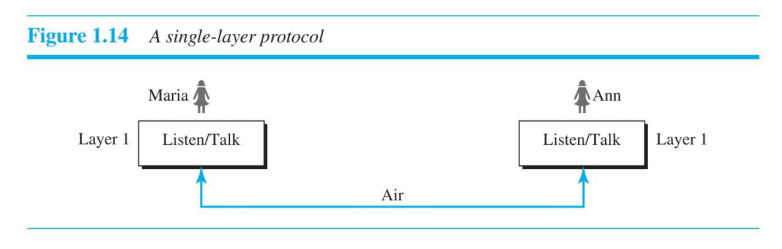


Figure 1.14 *A single-layer protocol*

2. A THREE-layer protocol (2 friends communicating with each other via MAIL) :-

Few examples of rules -

a. Greet the other person at the beginning of the letter.

b. Use proper words.

c. Bid farewell to the other person at the end of the letter.

Let's assume that both of them have 3 ROBOTS to facilitate the communication -

A. At the sender's end -

a. The layer 3 robot LISTENS to the speaker, WRITES the letter using speech-to-text and gives it to the layer 2 robot.

b. The layer 2 robot takes the letter from the layer 3 robot, ENCRYPTS it and gives the encrypted version to the layer 1 robot.

c. The layer 1 robot takes the encrypted letter from the layer 2 robot, wraps it into an ENVELOPE and gives it to the postman after writing the sender's and receiver's addresses.

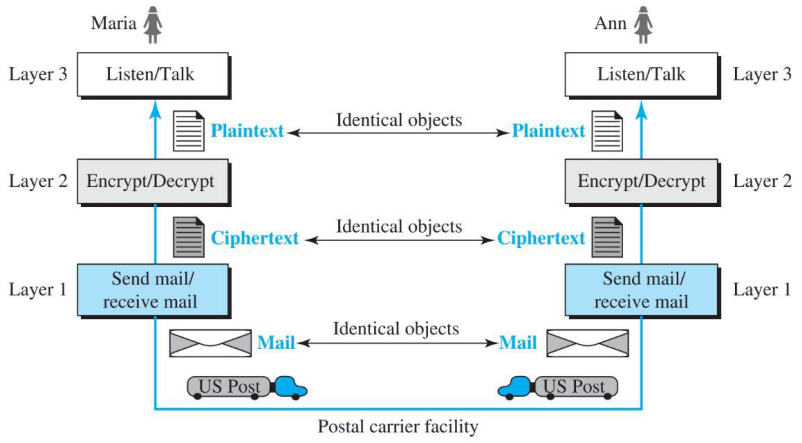
B. At the receiver's end –

c. The layer 1 robot takes the envelope from the postman, takes the encrypted letter out from the envelope and gives it to the layer 2 robot.

b. The layer 2 robot takes the encrypted letter from the layer 1 robot, DECRYPTS it and gives the decrypted version to the layer 3 robot.

a. The layer 3 robot takes the letter from the layer 2 robot and READS it aloud to the listener using text-to-speech.

Figure 1.15 *A three-layer protocol*



Protocol layering enables us to divide a COMPLEX task into several SMALLER and SIMPLER tasks.

For eg., if Maria and Ann later decide that their encryption/decryption algorithm is NOT secure enough, then they ONLY need to replace the layer 2 robot, instead of having to replace ALL 3 robots.

This is referred to as MODULARITY.

A LAYER (MODULE) can be defined as a BLACK BOX with INPUTS AND OUTPUTS, without concern about how it EXACTLY works.

For eg., Maria and Ann can buy the layer 2 robot from DIFFERENT manufacturers, as long as the 2 robots work the same.

Protocol layering allows us to separate the SERVICES from the IMPLEMENTATION. For eg., Maria may decide NOT to use the layer 3 robot and to instead do its job herself.

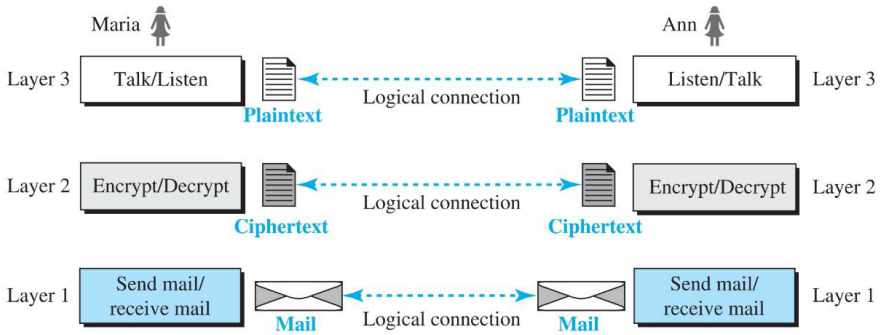
A layer needs to be able to RECEIVE services from the LOWER layers and to PROVIDE services to the UPPER layers.

Protocol layering also enables the INTERMEDIATE systems to use only SOME layers, instead of ALL.

PRINCIPLES of protocol layering –

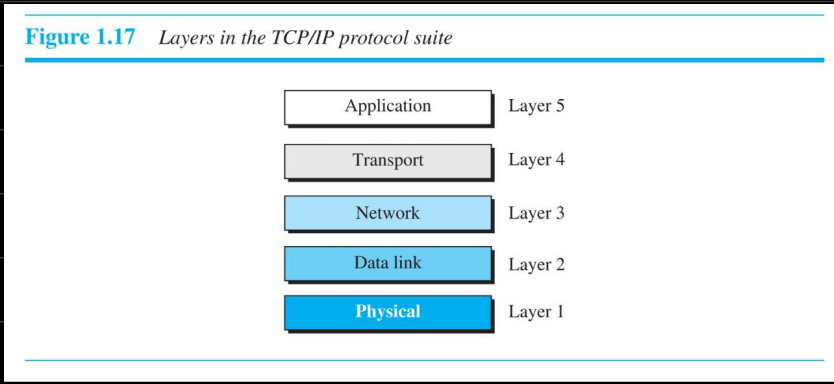
a. If we want BIDIRECTIONAL communication, then EACH layer must be able to perform two OPPOSITE tasks, one in each direction.
b. For EACH layer, the two OBJECTS (for eg., the letter) at both sites should be IDENTICAL.

Figure 1.16 *Logical connections between peer layers*

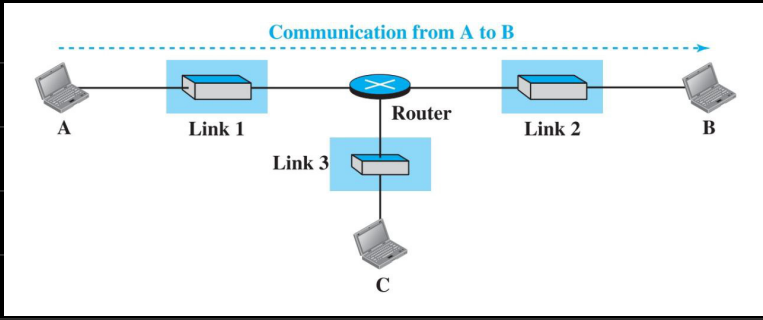


^ TCP/IP Protocol Suite

TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL (TCP/IP) is a protocol suite (a set of PROTOCOLS organized in different LAYERS) used in the Internet today.



Let there be 3 LANs (LINKS), each with a LINK-LAYER SWITCH, and the LANs be connected by 1 ROUTER.



Depending upon the context, the term LINK may refer to a CHANNEL or to a NETWORK.

Let host A communicate with host B.

Both the hosts will be involved in ALL 5 layers, because the SOURCE host will need to create a MESSAGE in the APPLICATION layer and send it DOWN the layers so that it is PHYSICALLY sent to the DESTINATION host, and the DESTINATION host will need to receive the MESSAGE at the PHYSICAL layer and then deliver it through the other layers to the APPLICATION layer.

The ROUTER will be involved ONLY in 3 layers as long as it is used ONLY for routing.
Although a router will always be invoved in ONLY 1 NETWORK layer, it will be involved in n DATA LINK and PHYSICAL layers, one for each LINK the router is connected to.
This is because each LINK may use its own DATA LINK or PHYSICAL protocol.

The LINK-LAYER SWITCHES will be involved ONLY in 2 layers.
Unlike the ROUTER, the LINK-LAYER SWITCHES will be involved in ONLY 1 DATA LINK layer and ONLY 1 PHYSICAL layer, as connections in the SAME link use the SAME set of protocols.

Figure 1.18 *Communication through an internet*

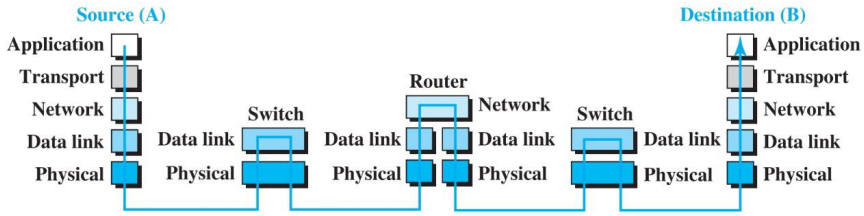
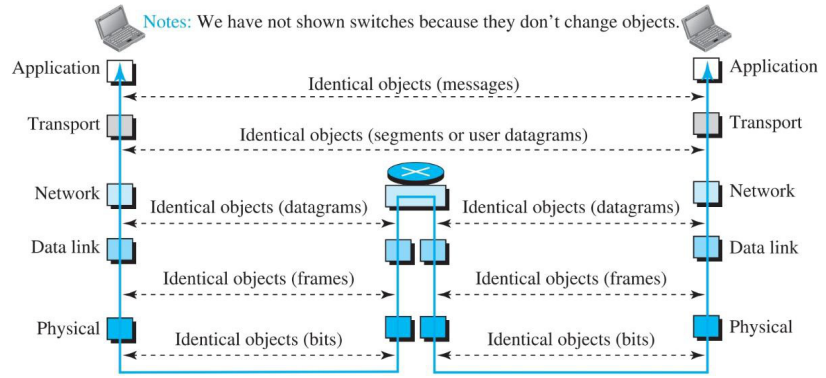


Figure 1.20 *Identical objects in the TCP/IP protocol suite*



Identical objects MAY NOT exist between the NETWORK, DATA LINK and PHYSICAL layers of the end HOSTS due to FRAGMENTATION, etc.

NETWORK layer's object (DATAGRAM) is aka a PACKET.

The duty of the APPLICATION, TRANSPORT and NETWORK layers is END-TO-END/HOST-TO-HOST, and their domain of duty is the INTERNET.
The duty of the DATA LINK and PHYSICAL layers is HOP-TO-HOP/NODE-TO-NODE, and their domain of duty is the LINK.

^ The OSI Model

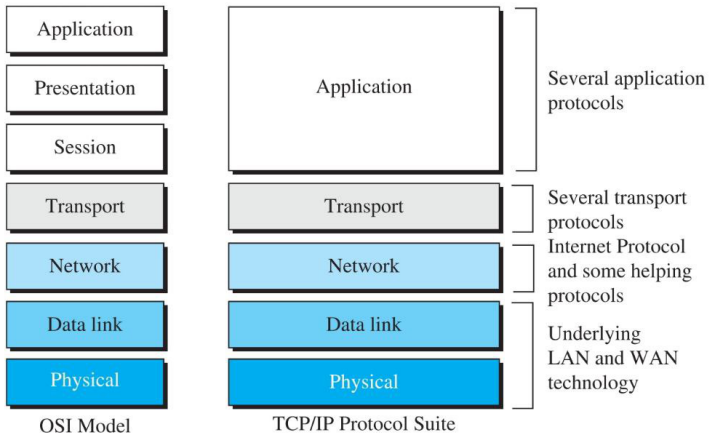
The TCP/IP protocol suite is NOT the only suite of protocols defined.

The OSI (OPEN SYSTEMS INTERCONNECTION) model is an ISO (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION) standard that covers all aspects of network communications.

Strictly speaking, the OSI model is NOT a set of protocols, and is rather a MODEL for UNDERSTANDING and DESIGNING a network architecture that is FLEXIBLE, ROBUST and INTEROPERABLE.

The OSI model was intended to be the BASIS for the creation of a new set of PROTOCOLS.

Figure 1.22 *TCP/IP and OSI model*



The PRESENTATION and the SESSION layers were not added to the TCP/IP protocol suite because some of the functionalities of the SESSION layer were ALREADY available in some of the TRANSPORT layer protocols of the TCP/IP protocol suite, and the other functionalities of the PRESENTATION and the SESSION layers can be easily included in the APPLICATION layer of the TCP/IP protocol suite.

Even though the OSI model appeared AFTER the TCP/IP protocol suite, the former could NOT replace the latter because

1. OSI was completed when TCP/IP was FULLY in place and a LOT of time and money had already been spent on the suite.
2. Some layers in OSI such as PRESENTATION and SESSION were NEVER fully defined.
3. OSI did NOT show a high enough level of PERFORMANCE as compared to TCP/IP.