Short notes on Computer Networks and Data Communication

Topics:
Introduction: An overview of networks
the Internet, services, and protocols
RFCs and standards of networking
Circuit Switching, Packet Switching
Layered Network Architecture: Overview of the TCP/IP Network, OSI Layers

INTRODUCTION

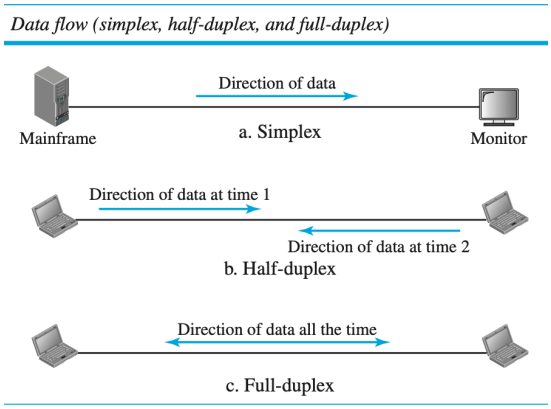
DATA COMMUNICATIONS

Data communications are the exchange of data between two devices via a transmission medium, such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system comprising a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. Delivery. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. Accuracy. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. Timeliness. The system must deliver data promptly. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. **Jitter**. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with a 30-ms delay and others with a 40-ms delay, an uneven quality in the video is the result.

DATA FLOW

Communication between two devices can be simplex, half-duplex, or full-duplex, as shown in the Figure below.



1. Simplex
   In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive
   Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.
2. Half-Duplex
   In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device sends, the other can only receive, and vice versa. Walkie-talkies and CB (citizen band) radios are both half-duplex systems.
3. Full-Duplex
   In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously. In full-duplex mode, signals in one direction share the link's capacity with signals in another. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending

and the other for receiving, or the channel's capacity is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people communicate by a telephone line, both can talk and listen simultaneously.

NETWORKS

A network is the interconnection of a set of devices capable of communication. In this definition, a device can be a host (or an end system as it is sometimes called) such as a large computer, desktop, laptop, workstation, cellular phone, or security system or can also be a connecting device such as a router, which connects the network to other networks, a switch, which connects devices together, a modem (modulator-demodulator), which changes the form of data, and so on. These devices in a network are connected using wired or wireless transmission media such as cable or air.

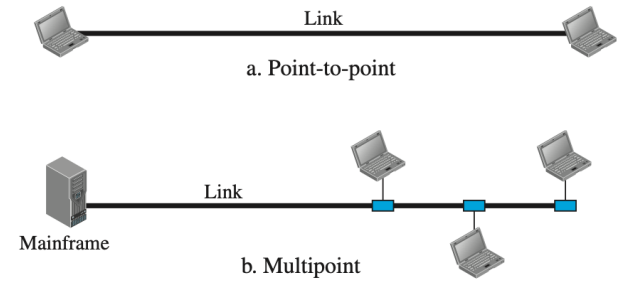
TYPE OF CONNECTION

1. Point-to-Point

   A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When we change television channels by infrared remote control, we establish a point-to-point connection between the remote control and the television's control system.
2. Multipoint

   A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.

Types of connections: point-to-point and multipoint



TOPOLOGIES

1. Mesh Topology

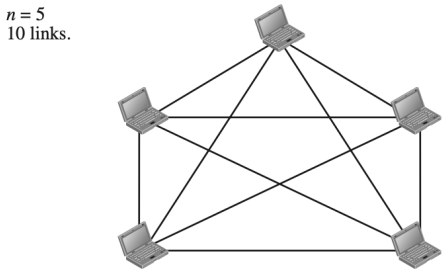
   In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.
2. Star Topology

   In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange.
3. Bus Topology

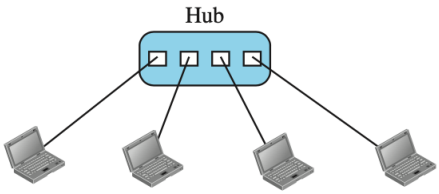
   The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network
4. Ring Topology

   In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

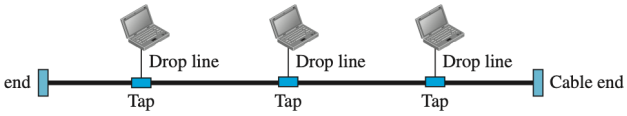
A fully connected mesh topology (five devices)



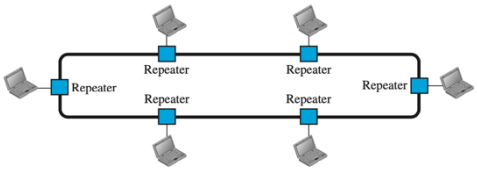
A star topology connecting four stations



A bus topology connecting three stations



A ring topology connecting six stations

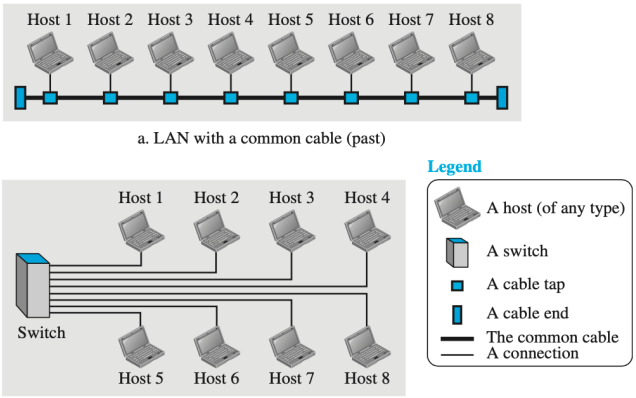


NETWORK TYPES

1. Local Area Network

A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus. Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include audio and video devices. Each host in a LAN has an identifier -an address, that uniquely defines the host in the LAN.

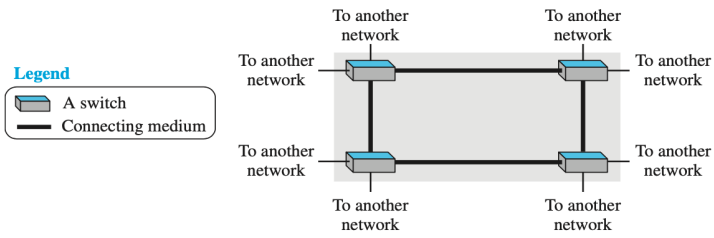
An isolated LAN in the past and today



2. Wide Area Network

A wide area network (WAN) is also an interconnection of devices capable of communication. However, there are some differences between a LAN and a WAN. A LAN is normally limited in size, spanning an office, a building, or a campus; a WAN has a wider geographical span, spanning a town, a state, a country, or even the world. *A LAN interconnects hosts*; a WAN interconnects connecting devices such as switches, routers, or modems. A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.

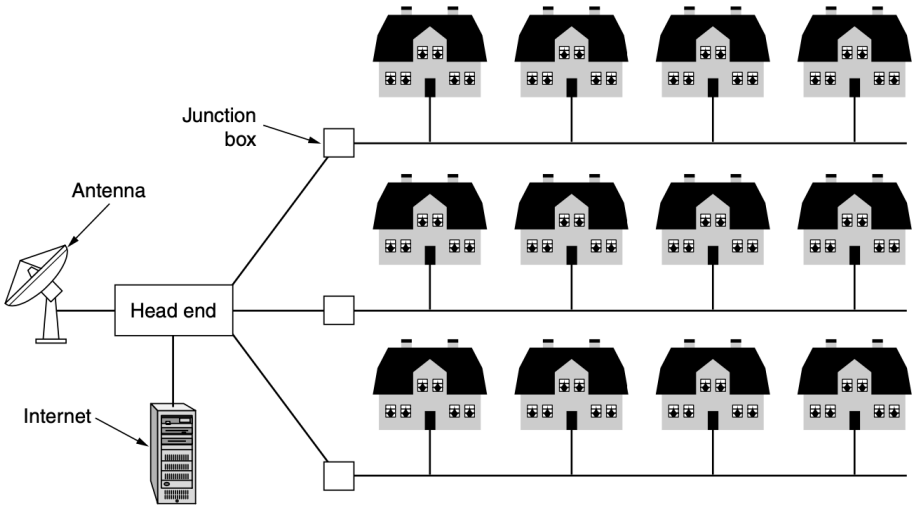
A switched WAN



3. Metropolitan Area Networks

A MAN (Metropolitan Area Network) covers a city. The best-known examples of MANs are the cable television networks available in many cities. These systems grew from earlier community antenna systems

used in poor over-the-air television reception areas. In those early systems, a large antenna was placed on top of a nearby hill, and a signal was then piped to the subscribers' houses.



4. Internetwork

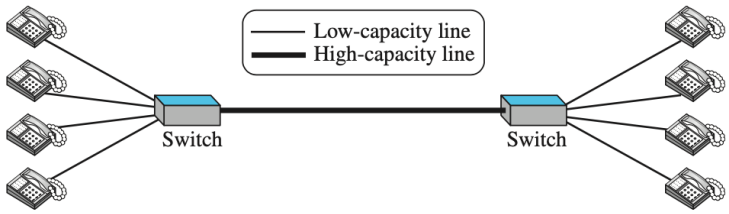
Today, it is very rare to see a LAN or a WAN in isolation; they are connected to one another. When two or more networks are connected, they make an internetwork or internet.

An internet is a switched network in which a switch connects at least two links together. A switch must forward data from one network to another when required. The two most common types of switched networks are *circuit-switched* and *packet-switched* networks.

a) Circuit-Switched Network

In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive. We have used telephone sets instead of computers as an end system because circuit switching was very common in telephone networks in the past, although part of the telephone network today is a packet-switched network.

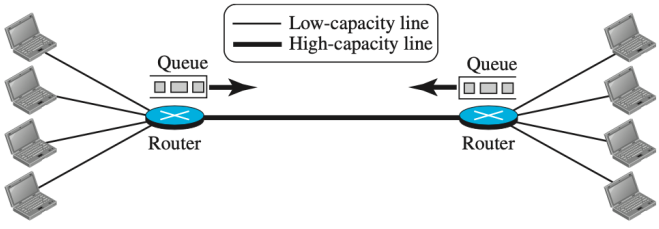
A circuit-switched network



b) Packet-Switched Network

In a computer network, the communication between the two ends is done in blocks of data called *packets*. In other words, instead of the continuous communication we see between two telephone sets when they are being used, we see the exchange of individual data packets between the two computers. This allows us to make the switches function *for both storing and forwarding* because a packet is an independent entity that can be stored and sent later.

A packet-switched network

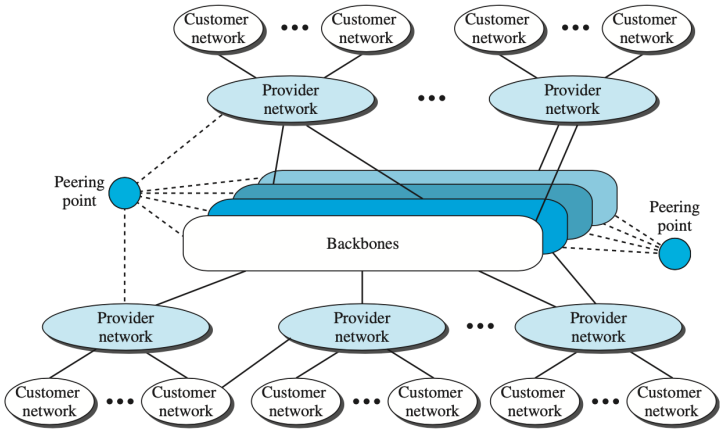


The Internet

As we discussed before, the internet is two or more networks that can communicate with each other. *The internet* is the most notable, which is composed of thousands of interconnected networks.

Several services are provided by the Internet. Users pay fees to provider networks for receiving services. Backbones and provider networks are also called Internet Service Providers (ISPs). The backbones are often called international ISPs; the provider networks are often called national or regional ISPs.

The Internet today



INTERNET STANDARDS

An Internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a six-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a *Request for Comment* (RFC). Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

The Internet Engineering Task Force (IETF) is a forum of working groups managed by the Internet Engineering Steering Group (IESG). IETF is responsible for identifying operational problems and proposing solutions to these problems. IETF also develops and reviews specifications intended as Internet standards.

PROTOCOLS AND SERVICES BASICS

In data communication and networking, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively. We may need to divide the rules between different layers, in which case we need a protocol at each layer or protocol layering. Layers can offer two different types of service to the layers above them: *connection-oriented* and *connectionless*.

Connection-oriented service is modeled after the telephone system. To talk to someone, you pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.

In contrast, **connectionless service** is modeled after the postal system. Each message (letter) carries the full destination address and is routed through the intermediate nodes inside the system independent of all subsequent messages.

TCP/IP PROTOCOL SUITE

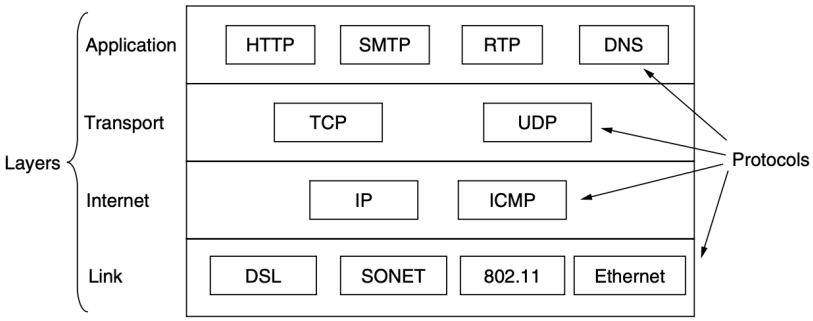
The ARPANET was a research network sponsored by the DoD (U.S. Department of Defense). It eventually connected hundreds of universities and government institutions using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so a new reference architecture was needed. Thus, from nearly the beginning, the ability to connect multiple networks in a seamless way was one of the major design goals. This architecture later became known as the TCP/IP Reference Model after its two primary protocols.

a) The Link Layer
All these requirements led to choosing a packet-switching network based on a connectionless layer that runs across different networks. The lowest layer in the model, the link layer, describes what links such as serial lines and classic Internet must do to meet the needs of this connectionless Internet layer.

b) The Internet Layer
The internet layer is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them if in-order delivery is desired.

c) The Transport Layer
The layer above the internet layer in the TCP/IP model is now usually called the transport layer. It allows peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol. The second, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.

d) The Application Layer
On top of the transport layer is the application layer. It contains all the high-level protocols. The early ones included virtual terminals (TELNET), file transfer (FTP), and electronic mail (SMTP). Many other protocols have been added to these over the years.



THE OSI MODEL

The *International Organization for Standardization* (ISO) is a multinational body dedicated to worldwide international standards agreements. Almost three-fourths of the countries in the world are represented in the ISO. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s. This model has 7 layers:

a) The Physical Layer
The physical layer is concerned with transmitting raw bits over a communication channel. The design issues involve ensuring that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions here are what electrical signals should be used to represent a 1 and a 0, how many nanoseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established, how it is torn down when both sides are finished, how many pins the network connector has, and what each pin is used for.

b) The Data Link Layer
The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors. It does so by masking the real errors so the network layer does not see them. It accomplishes this task by having the sender break up the input data into *data frames* (typically a few hundred or a few thousand bytes) and transmit the frames sequentially.
Broadcast networks have an additional issue in the data link layer: controlling access to the shared channel. A special sublayer of the data link layer, the medium access control sublayer, deals with this problem.

c) The Network Layer
The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. If too many packets are present in the subnet simultaneously,

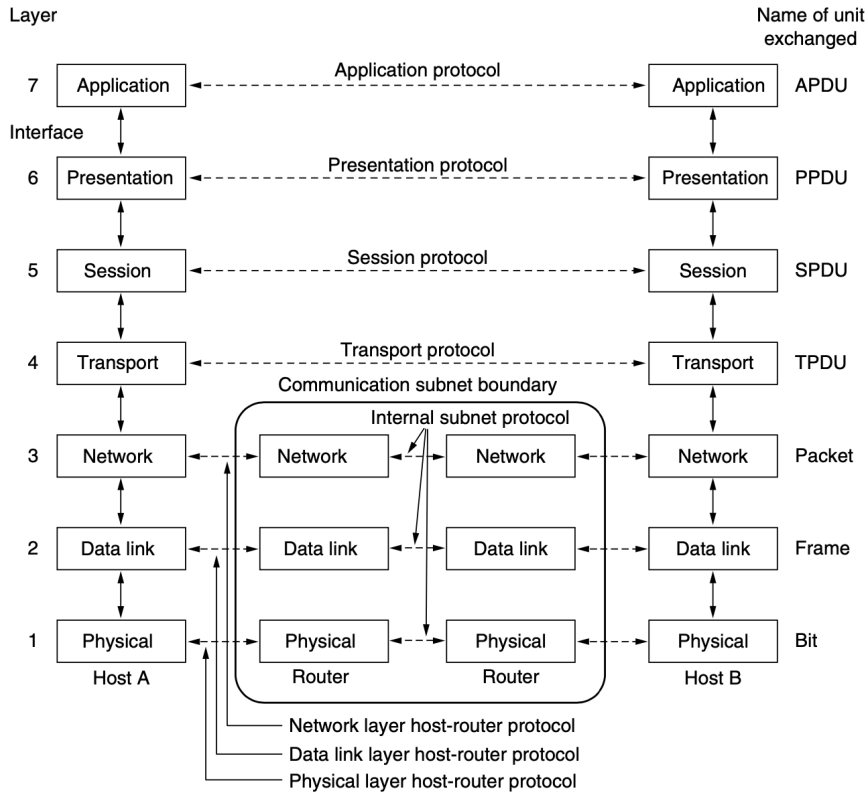
they will get in one another's way, forming bottlenecks. Handling congestion is also a responsibility of the network layer, in conjunction with higher layers that adapt to the load.

d) The Transport Layer
The basic function of the transport layer is to accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology over the course of time.
The transport layer also determines what type of service to provide to the session layer and, ultimately, to the network users.

e) The Session Layer
The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation simultaneously), and synchronization (checkpointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

f) The Presentation Layer
Unlike the lower layers, which are mostly concerned with moving bits around, the presentation layer is concerned with the syntax and semantics of the information transmitted. To make it possible for computers with different internal data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used ''on the wire.''

g) The Application Layer
The application layer contains a variety of protocols that users commonly need. One widely used application protocol is HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server hosting it using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.



COMMUNICATION AND COMPARISON OF LAYERS

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols. Also, the functionality of the layers is roughly similar. For example, in both models, the layers up through and including the transport layer are there to provide an end-to-end, network-independent transport service to processes wishing to communicate.

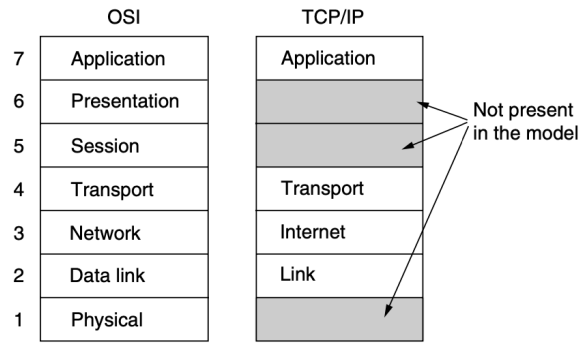
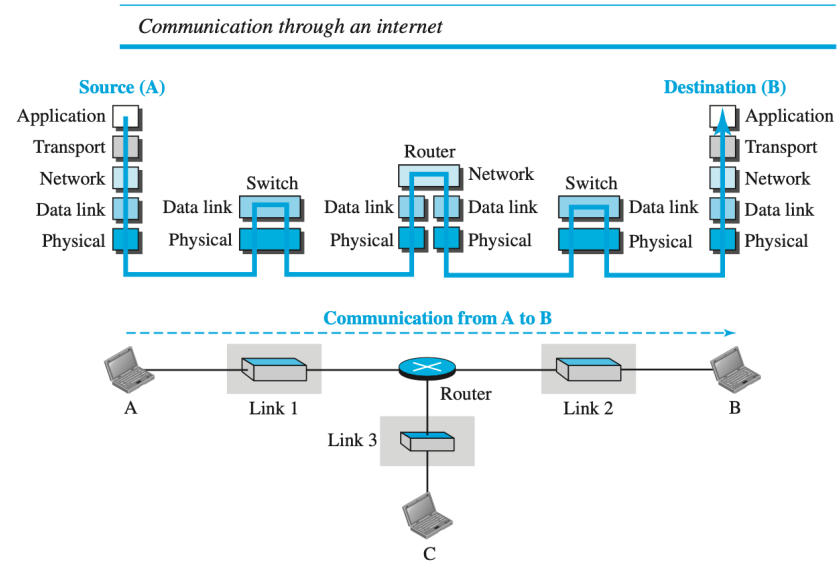


Figure 1-21. The TCP/IP reference model.

The layers in the network communicate logically between themselves. As per the need, not all devices necessarily implement all the layers in the model.



References:

1. Andrew S. Tanenbaum, Computer Networks 5th Edition, Pearson, 2013, 978- 9332518742
2. Behrouz Forouzan, Data Communications & Networking Tata McGraw Hill, 2006, ISBN 978-0070584082