Network Hardware

1.3 Introduction:

There are two types of transmission technology that are widely used: broadcast links and point-to-point links.

Point-to-point links connect individual pairs of machines. Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

In contrast, on a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored. A wireless network is a common example of a broadcast link, with communication shared over a coverage region that depends on the wireless channel and the transmitting machine.

In Table 1.1 we classify multiple processor systems (networks) by their rough physical size.

<table>
<thead>
<tr>
<th>Interprocessor distance</th>
<th>Processors located in same</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 m</td>
<td>Square meter</td>
<td>Personal area network</td>
</tr>
<tr>
<td>10 m</td>
<td>Room</td>
<td>Local area network</td>
</tr>
<tr>
<td>100 m</td>
<td>Building</td>
<td>Local area network</td>
</tr>
<tr>
<td>1 km</td>
<td>Campus</td>
<td>Local area network</td>
</tr>
<tr>
<td>10 km</td>
<td>City</td>
<td>Metropolitan area network</td>
</tr>
<tr>
<td>100 km</td>
<td>Country</td>
<td>Wide area network</td>
</tr>
<tr>
<td>1000 km</td>
<td>Continent</td>
<td>Wide area network</td>
</tr>
<tr>
<td>10,000 km</td>
<td>Planet</td>
<td>The internet</td>
</tr>
</tbody>
</table>

1.3.1 Personal Area Network (PAN)

PANs let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables. Some companies got together to design a short-range wireless network called Bluetooth to connect these components without wires.

In the simplest form, Bluetooth networks use the master-slave model of Fig. 1.4. The system unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves. The
master tells the slaves what addresses to use, when they can broadcast, how long they can transmit, what frequencies they can use, and so on.

![Bluetooth PAN configuration](image)

**Fig. 1.4:** Bluetooth PAN configuration.

### 1.3.2 Local Area Networks (LANs)

A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information. When LANs are used by companies, they are called **enterprise networks**.

Wireless LANs are very popular these days, especially in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables. In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers. In most cases, each computer talks to a device in the ceiling as shown in Fig. 1.5 (a). This device, called an **AP (Access Point), wireless router, or base station**, relays packets between the wireless computers and also between them and the Internet. However, if other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration.

There is a standard for wireless LANs called **IEEE 802.11**, popularly known as **WiFi**, which has become very widespread. It runs at speeds anywhere from 11 to hundreds of Mbps.

Wired LANs use a range of different transmission technologies. Most of them use copper wires, but some use optical fibre. Typically, wired LANs run at speeds of 100 Mbps to 1 or even 10 Gbps in newer LANs.

The topology of many wired LANs is built from point-to-point links. IEEE 802.3, popularly called **Ethernet**, is, by far, the most common type of wired LAN. Fig. 1.5 (b) shows a sample topology of **switched Ethernet**. Each computer speaks the Ethernet protocol and connects to a box called a **switch** with a point-to-point link.
In short, home LANs offer many opportunities and challenges. Most of the latter relate to the need for the networks to be easy to manage, dependable, and secure, especially in the hands of nontechnical users, as well as low cost.

![Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.](image)

**Fig. 1.5:** Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

### 1.3.3 Metropolitan Area Networks (MANs)

A MAN covers a city. The best-known examples of MANs are the cable television networks available in many cities. Generally, a MAN might look something like the system shown in **Fig. 1.6**. In this figure we see both television signals and Internet being fed into the centralized cable headend for subsequent distribution to people’s homes.

Cable television is not the only MAN, though. Recent developments in highspeed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as **WiMAX**.

![A metropolitan area network based on cable TV.](image)

**Fig. 1.6:** A metropolitan area network based on cable TV.
1.3.4 Wide Area Networks (WANs)

A WAN spans a large geographical area, often a country or continent. We will begin our discussion with wired WANs, using the example of a company with branch offices in different cities.

The WAN in Fig. 1.7 is a network that connects offices in three cities. Each of these offices contains computers intended for running user (i.e., application) programs. These machines can be called as hosts. The rest of the network that connects these hosts is then called the communication subnet, or just subnet for short. The job of the subnet is to carry messages from host to host. In most WANs, the subnet consists of two distinct components: transmission lines and switching elements.

Transmission lines: move bits between machines. They can be made of copper wire, optical fibre, or even radio links.

Switching elements, or just switches, are specialized computers that connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them. These switching computers have been called by various names in the past; the name router is now most commonly used. The network selects the data path according to a specific routing algorithm. Many such algorithms exist.

Hence, the “subnet” is a collection of routers and communication lines that moved packets from the source host to the destination host.

The subnet operator is known as a network service provider and the computers users are its customers. In the Internet network the subnet operator is called an ISP (Internet Service Provider) and the subnet is an ISP network.

Other kinds of WANs make heavy use of wireless technologies. In satellite systems, each computer on the ground has an antenna through which it can send data to and receive data from to a satellite in orbit. The cellular telephone network is another example of a WAN that uses wireless technology.
1.3.5 Internetworks

A collection of interconnected networks is called an **internetwork or internet**. These terms will be used in a generic sense, in contrast to the worldwide Internet (which is one specific internet), which is always capitalize. The Internet uses ISP networks to connect enterprise networks, home networks, and many other networks.

Generally, connecting a LAN and a WAN or connecting two LANs is the usual way to form an internetwork.

Further, the general name for a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is a **gateway**.

1.4 Network Software; Protocol Hierarchies

To reduce their design complexity, most networks are organized as a stack of layers or levels. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

When layer $n$ on one machine carries on a conversation with layer $n$ on another machine, the rules and conventions used in this conversation are collectively known as the layer $n$ **protocol**.

A **protocol** is an agreement between the communicating parties on how communication is to proceed.

Let us take an example, a five-layer network as illustrated in Fig. 1.8.

![Diagram of a five-layer network](image)

**Fig. 1.8:** Layers, protocols, and interfaces.

Below layer 1 is the **physical medium** through which actual communication occurs. Between each pair of adjacent layers is an **interface**. The interface defines which primitive operations
and services the lower layer makes available to the upper one. A set of layers and protocols is called **network architecture**.

A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack**.

**Now consider a more technical example**: how to provide communication to the top layer of the five-layer network in Fig. 1.9. A message, $M$, is produced by an application process running in layer 5 and given to layer 4 for transmission.

Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3. The header includes control information, such as addresses, to allow layer 4 on the destination machine to deliver the message. Other examples of control information used in some layers are sequence numbers (in case the lower layer does not preserve message order), sizes, and times.

In many networks, no limit is placed on the size of messages transmitted in the layer 4 protocol but there is nearly always a limit imposed by the layer 3 protocol. Consequently, layer 3 must break up the incoming messages into smaller units, packets, prepending a layer 3 header to each packet. In this example, $M$ is split into two parts, $M_1$ and $M_2$, that will be transmitted separately.

Layer 3 decides which of the outgoing lines to use and passes the packets to layer 2. Layer 2 adds to each piece not only a header but also a trailer, and gives the resulting unit to layer 1 for physical transmission. At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses. None of the headers for layers below $n$ are passed up to layer $n$.

---

**Fig. 1.9**: Example information flow supporting virtual communication in layer 5.
1.5 Reference Models

In this section we will discuss two important network architectures: the **Open Systems Interconnection (OSI)** reference model and the **Transmission Control Protocol/Internet Protocol (TCP/IP)** reference model. Although the protocols associated with the OSI model are not used any more, the model itself is actually quite general and still valid, and the features discussed at each layer are still very important.

The TCP/IP model has the opposite properties: the model itself is not of much use but the protocols are widely used. For this reason we will look at both of them in detail.

1.5.1 The OSI Reference Model

The OSI model is shown in Fig. 1.10. This model is based on a proposal developed by the **International Standards Organization (ISO)** as a first step toward international standardization of the protocols used in the various layers (1983) and it was revised in 1995.

The model is called the ISO OSI Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

The OSI model has seven layers. The OSI model tells what each layer should do. Below we will discuss each layer of the model in turn, starting at the bottom layer.

![OSI Reference Model Diagram](diagram.png)

*Fig. 1.10: The OSI reference model (PDU: Protocol Data Unit)*
The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure 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 many pins the network connector has, and what each pin is used for. These design issues largely deal with mechanical, electrical, and timing interfaces, as well as the physical transmission medium, which lies below the physical layer.

The Data Link Layer

The Data-Link layer contains two sub-layers that are described in the IEEE-802 LAN standards:

- Media Access Control (MAC)
- Logical Link Control (LLC)

The Data-Link layer ensures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully. It also ensures that incoming data has been received successfully by analysing bit patterns at special places in the frames.

Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism may be needed to let the transmitter know when the receiver can accept more data.

Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel.

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. Routes can be based on static tables that are “wired into” the network and rarely changed, or more often they can be updated automatically to avoid failed components. They can also be determined at the start of each conversation, for example, a terminal session, such as a login to a remote machine. Finally, they can be highly dynamic, being determined anew for each packet to reflect the current network load.

If too many packets are present in the subnet at the same time, 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 the load they place on the network. More generally, the quality of service provided (delay, transit time) is also a network layer issue.

When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from that used by the first one. The second one may not accept the packet at all because it is too large.
The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

**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 unavoidable changes in the hardware technology over the time sequence.

The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network.

The transport layer is a true end-to-end layer; it carries data all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers, each protocol is between a machine and its immediate neighbours, and not between the ultimate source and destination machines, which may be separated by many routers. The difference between layers 1 through 3, which are chained, and layers 4 through 7, which are end-to-end, is illustrated in Fig. 1.10.

**The Session Layer**

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control, token management (preventing two parties from attempting the same critical operation simultaneously), and synchronization.

**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. In order 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.” The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records) to be defined and exchanged.

**The Application Layer**

The application layer contains a variety of protocols that are commonly needed by users. 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 the page using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.
1.5.2 The TCP/IP Reference Model

Let us now turn from the OSI reference model to the reference model used in the grandparent of all wide area computer networks, the ARPANET, and its successor, the worldwide Internet. Although we will give a brief history of the ARPANET later, it is useful to mention a few key aspects of it now. The ARPANET was a research network sponsored by the DoD (U.S. Department of Defence). It eventually connected hundreds of universities and government installations, using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so 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.

The Link Layer

It is a combination of the Data Link and Physical layers of the OSI model which consists of the actual hardware. This includes wires, network interface cards, etc. Other related details within this layer are connectors, signal strength, and wavelength along with various others. It will use the required LAN operating algorithms and it is responsible for placing the data within a frame. The frame is the package that holds the data, in the same way as an envelope holds a letter. The frame holds the hardware address of the host and checking algorithms for data integrity. This layer has actually not been specified in details because it depends on which technology is being used such as Ethernet.

The Internet Layer

The routing and delivery of data is the responsibility of this layer and is the key component of this architecture. It allows communication across networks of the same and different types and carries out translations to deal with dissimilar data addressing schemes. It injects packets into any network and deliver them to the destination independently to one another. Because the path through the network is not predetermined, the packets may be received out of order. The upper layers are responsible for the reordering of the data. This layer can be compared to the network layer of the OSI model.

The internet layer defines an official packet format using protocol called IP (Internet Protocol), plus a companion protocol called ICMP (Internet Control Message Protocol).

![Fig. 1.11: The TCP/IP reference model.](image-url)
The Transport Layer

This layer acts as the delivery service used by the application layer. It uses the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The choice is made based on the application's transmission reliability requirements. The TCP, is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It segments the incoming byte stream into discrete messages and passes each one on to the internet layer. At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

The second protocol in this layer, UDP (User Datagram Protocol), is unreliable, connectionless protocols for applications that do not want TCP’s sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig. 1.12. Since the model was developed, IP has been implemented on many other networks. The transport layer also handles all error detection and recovery. It uses checksums, acknowledgements, and timeouts to control transmissions and end to end verification. Unlike the OSI model, TCP/IP treats reliability as an end-to-end problem.

The Application Layer

The TCP/IP model does not have session or presentation layers. Instead, applications simply include any session and presentation functions that they require. Experience with the OSI model has proven this view correct: these layers are of little use to most applications.

On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included file transfer (FTP), and electronic mail, Simple Mail Transfer Protocol (SMTP). Many other protocols have been added to these over the years. Some important ones, shown in Fig. 1.12, include the Domain Name System (DNS), for mapping host names onto their network addresses, HTTP, the protocol for fetching pages on the World Wide Web, and RTP, the protocol for delivering real-time media such as voice or movies.

Fig. 1.12: The TCP/IP model with some protocols.