TRANSMISSION MEDIA

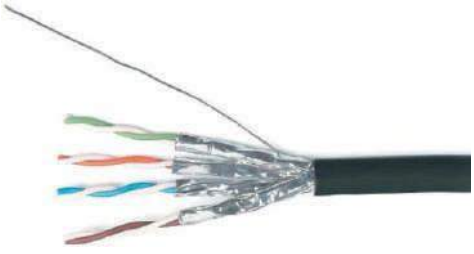
Computers must be connected to each other to form a network. Computers can be connected using wires/cables or they can be connected in a wireless manner.

Wired Transmission Media

There are various types of cables that can be used for setting up a network. Some of them are discussed here.

← **Twisted Pair Cable:** It consists of a pair of insulated wires twisted together. The use of two wires twisted around each other helps to reduce disturbances in the signals.

The **twisted pair cable** is often used in two or more pairs, all within a single cable. Twisted pair cabling comes in two varieties—shielded (**Shielded Twisted Pair** or **STP**) and unshielded (**Unshielded Twisted Pair** or **UTP**). UTP cable is the most commonly used cable in computer networking.



Coaxial Cable (coax): **Coaxial cable** is an electrical cable with a conductor at its centre (Fig. 1.13). The inner conductor is surrounded by a tubular insulating layer. The insulating layer is surrounded by a conductive layer called the shield, which is finally covered with a thin insulating layer on the outside.

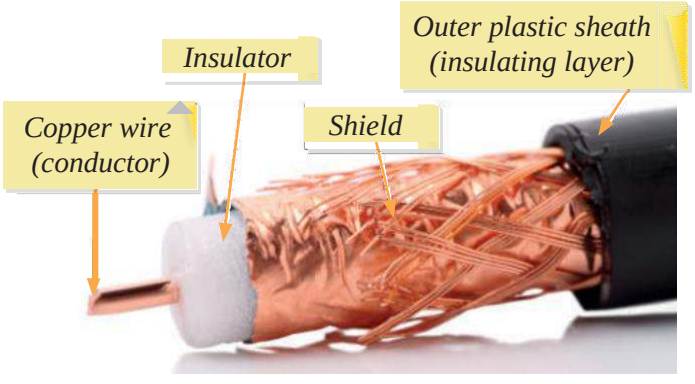


Fig. 1.13 *Coaxial wire*

← **Optical Fibre Cable:** **Optical fibre cable** consists of a central glass core surrounded by several layers of protective material (Fig. 1.14). It transmits data in the form of light rather than electronic signals, thus eliminating the problem of electrical interference. Fibre optic cable is expensive as

compared to coaxial and twisted pair cables but can transmit signals over much longer distances. It also has the capability to carry data at a very high speed.

Wireless Transmission Media

In wireless networks, data is transmitted without wires. Some of the ways in which wireless networks may be set up are as follows.

← **Infrared:** The **infrared communication** range of the devices communicating through infrared waves is very limited. **Infrared waves** cannot penetrate walls or other obstructions and so there should be no physical barrier between the communicating devices. The communication between a TV set and a remote control happens through infrared waves. Infrared mouse and keyboard are other examples of devices that make use of infrared waves for data transmission.

← **Microwave Transmission:** **Microwave communications** are unidirectional. They can be used for terrestrial communication (on the surface of the earth) or for satellite communication.

Microwave propagation is line-of-sight communication. So, when used for terrestrial communication, the towers with antennas mounted on them need to be in direct sight of each other. The antennas are usually located at substantial heights above the ground level to extend the range between antennas and to be able to transmit over obstacles. You must have noticed high towers with microwave antennas in your city.

Microwaves can pass through the earth's atmosphere easily and can be used to transmit information between satellites and the earth's base station (Fig. 1.15).

Fig. 1.15 *Microwave transmission*

Fig. 1.16 *Microwave antenna*

← **Radiowave Transmission:** **Radiowave communications** are omnidirectional, which means that they travel in all directions from the source, so that the transmitter and receiver do not have to be carefully aligned physically. Radio waves are easy to generate, can travel long distances and penetrate through buildings easily. So they are widely used for communication both indoors and outdoors (Fig. 1.17). However, at all frequencies, radio waves are subject to interference from motors and other electrical equipment.

Fig. 1.17 *Radiowave antenna*

Bluetooth and Wi-Fi are both wireless technologies that use radio frequency waves to create networks.

← **Bluetooth technology** is used for exchanging data over short distances using radio waves. This technology uses low power, has a short range [30 feet (approx.)] and medium transmission speed. Bluetooth technology can be used to transfer songs or pictures between two mobile phones or a Bluetooth headset can be used with a mobile phone.

WiFi technology also makes use of radio waves to transmit and receive data. This technology requires more energy but enables the signal to go farther (300 feet approx.) with a faster rate of transmission. This technology is used to set up networks in which a computer's wireless adapter translates the data into a radio signal and transmits it. A wireless router receives the signal, decodes it and sends it to the Internet using a wired connection.

Fig. Wi Technology

← **WiMAX (Worldwide Interoperability for Microwave Access):** Its technology is similar to WiFi, but it operates at higher speeds and can cover greater distances and greater number of users as compared to WiFi.

Fig. WiMAX W

NETWORK DEVICES

Various devices are used for setting up a computer network. Let us discuss a few devices that play a crucial role in a computer network.

- **NIC (Network Interface Card):** It is a hardware device that is attached to a computer to enable it to communicate over the network (Fig.1.21). The **NIC** has a ROM chip that contains a unique number, which is the hardware address or the **Media Access Control (MAC)** address. This hardware address uniquely identifies a computer on the Network.

- **Modem (Modulator-demodulator):** It is an electronic device that converts the digital signals of a computer into an analog form so that they can travel over a telephone line (Fig. 1.22). At the destination, the receiving modem converts the analog signals back into their digital form so that the destination computer understands them.

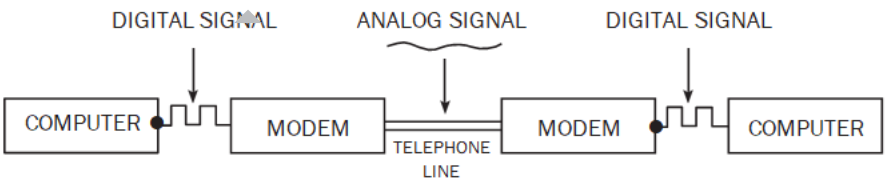


Fig. 1.22 *Transmission of signals through modem*

Modems are used for connecting computers to the Internet. Modems are connected to a computer and a telephone line (Fig. 1.24).

Fig. 1.23 *Modem*

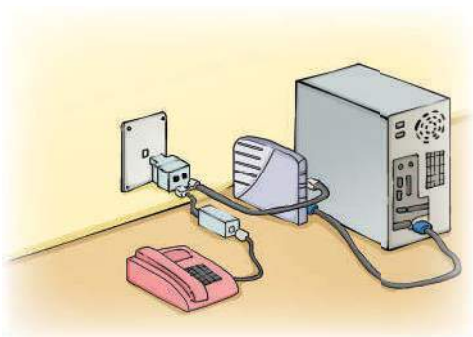


Fig. 1.24 *Connection of modem*

- **Hub:** A hub is a device that is used to connect computers in a network (Fig. 1.23). In a hub, when one computer sends data on the network, the hub simply forwards the packets to all the other computers connected to it (Fig. 1.26). Each computer is responsible for determining which packets are destined for it and which are to be ignored.

Fig. 1.25 *Hub*

Fig. 1.26 *Networking using a hub*

- **Switch:** A switch is a device that is also used to connect computers in a network (Fig. 1.27). However, a switch is a more intelligent device than a hub. Unlike a hub, the switch sends the incoming data to the desired destination only. It records the addresses of all the computers connected to it. So, when a packet is received, the switch reads the information about the destination address to determine if the destination device is connected to it or not. If the destination device is connected, the switch forwards the packet only to that destination device.

Fig. 1.27 *Switch*

  In this way, the other computers do not have to read and deal with data that is not meant for them.

Router: A router is a network device that connects two or more networks. It is commonly used to connect a computer or a network to the Internet.

Fig 8 *Router*

Lines from different networks are connected to a router. Wireless routers are also available. A router examines the address of the packet coming on the line, uses the routing information stored in it and forwards the packet to the next network. In this way, a packet after going through multiple routers reaches its destination.

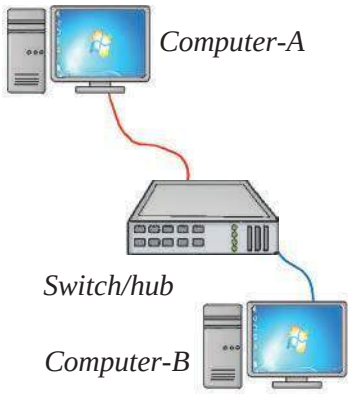
PROTOCOLS

Just the way we follow certain rules while communicating or travelling on the road, similarly rules or **protocols** have to be followed for effective network communication. Protocol is a set of rules used by computers on a network to communicate with each other. Some examples of protocols are:

- **HTTP (Hyper Text Transfer Protocol):** It is a protocol used between a web server and a web browser for transferring HTML pages.
- **TCP/IP (Transmission Control Protocol/Internet Protocol):** TCP is a protocol that is used along with the IP to send data over the Internet. The information is transmitted across the Internet in the form of bundles called **packets**. TCP is responsible for dividing the data into packets before they are sent and for reassembling the packets when they arrive at the destination. IP is a set of specifications that determines the best route for the packets across the Internet so that the packets reach their destination address.

PACKET SWITCHING IN NETWORKS

Let us explain the process of packet switching in a LAN. Suppose data has to be sent from Computer A to Computer B. The data at Computer A is split into small chunks, called **packets**. A header is added to every packet. The address of sender i.e. Computer A and address of receiver i.e. Computer B are put in the header. Then Computer A sends the packets to the switch. The switch has in-built software that



reads the header of each packet, determines the port at which the receiver is connected and forwards the packet on the corresponding cable (Fig. 1.29). Such a type of communication in which small units of data (or packets) are routed through a network, based on the destination address contained within each packet, is called **packet switching**.

When packets have to be sent to a computer on a different network, they pass through a number of routers. Every packet is numbered. Packets may follow different paths to reach the destination.

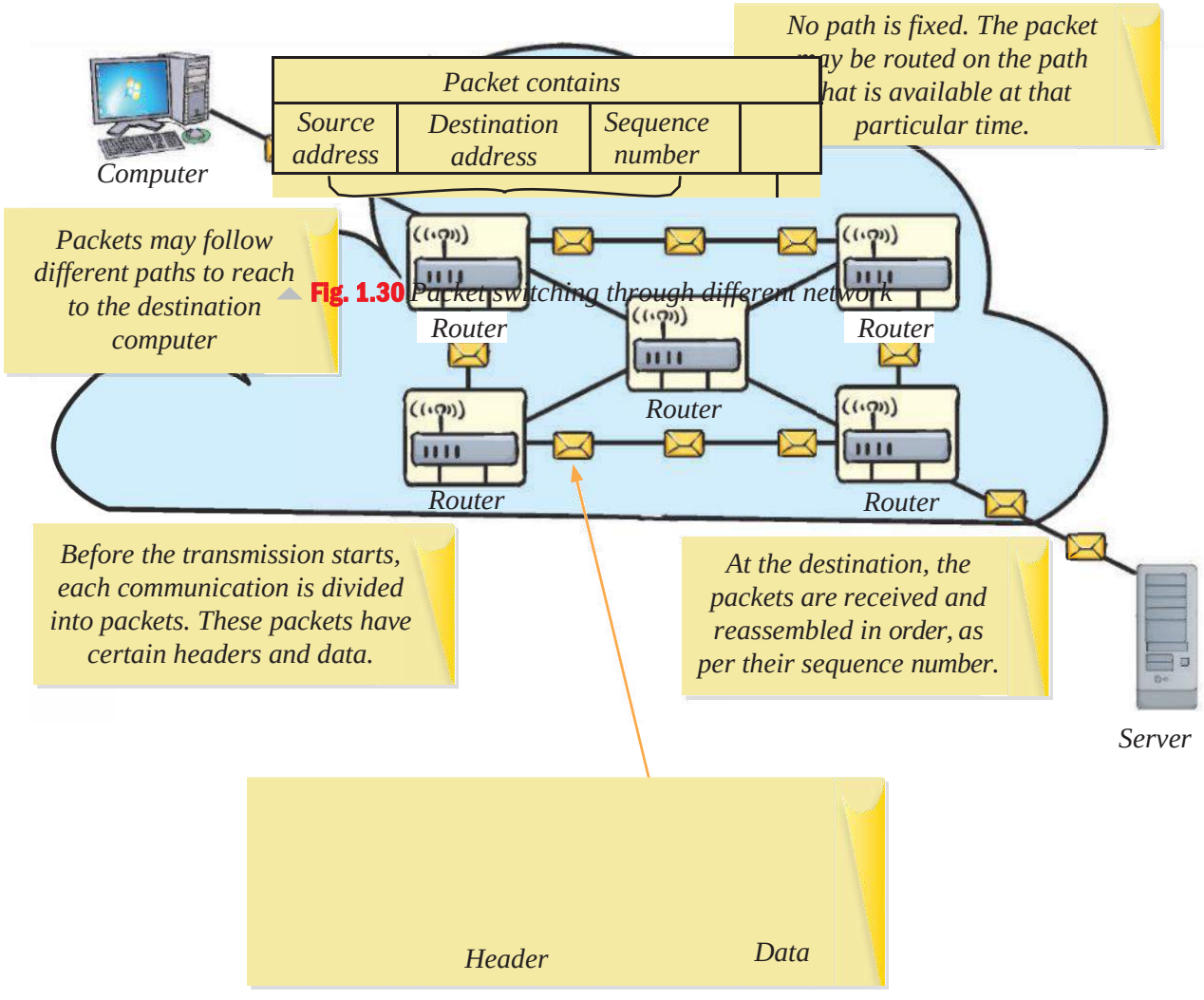


Fig. 1.30 *Packet switching through different network*

A computer on a network can be accessed by many users. Security measures have to be taken to protect networks from unauthorised access and to prevent data or information theft.

Threats to Computer

Files can be shared between the computers on a network. This makes a computer vulnerable to attacks by viruses, worms, Trojan horses and so on that can easily spread because of the underlying network. Let us discuss some of the common threats to computers.

- **Virus:** A **computer virus** spreads itself from one computer to another and interferes with the normal operations of a computer. Viruses attach themselves to any type of file and spread when these infected files are copied to other computers. People unknowingly spread a computer virus by sharing infected files or sending emails with viruses as attachments.

- **Worm:** A **worm** is a computer program that uses computer networks to send copies of itself to other computers on a network. A virus requires human action such as transferring of an infected file to spread itself. A worm can spread without any human action too. It replicates itself without the knowledge of the user. Worms can cause severe harm to a computer network such as blocking the network and reducing the speed of the network.

- **Trojan Horse:** A computer program that appears to be a useful software but actually causes damage once installed or executed onto your computer system is known as a **Trojan horse** or a **Trojan**. After getting installed, it allows unauthorised access to the computer. Trojan horses are very dangerous as they allow your computer to be remotely controlled by someone else and can cause loss of personal and confidential information (Fig. 1.31).

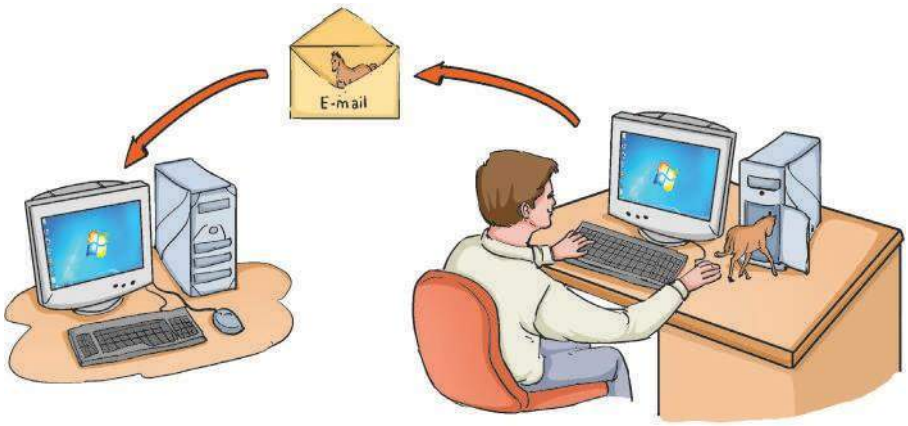


Fig 1 *People can install Trojans onto your computer or send it via email attachments*

Viruses, worms and Trojan horses may harm the data or affect the performance and the speed of a computer.

← **Data Theft:** It is a very serious problem for computer networks. People break into computer networks to either disrupt their functioning or to steal confidential information. **Hackers** are the computer experts who can break into computer systems and networks. There are two types of hackers—white hackers and black hackers.

White hackers study and break into networks to find and fix security loopholes. They offer their services to corporations, public organisations and educational institutions to make their networks more secure.

Black hackers or **crackers** have a criminal intention. Some examples are cracking bank accounts in order to transfer money to their own accounts, stealing confidential information and attacking the computer network of an organisation for money.

Computer Security

← **Antivirus Software:** Every computer on a computer network must have an **antivirus software** installed in it and it should be updated on a regular basis. Antivirus software can be used to protect the computer from various types of malware. Antivirus software can detect viruses, worms and so on, and warn you of their presence in your computer. It can also deactivate and clean up the computer of malicious software.

There are various types of antivirus software such as AVG, Avira, Norton and McAfee (Fig. 1.32).

▲ **Fig 1.32** *Logos of some antivirus software*

←**A** *Firewall:* **firewall** is used to prevent unauthorised access to a computer network. A firewall can be implemented as a software, a hardware or a combination of both. All data or messages entering or leaving a computer network pass through a firewall (Fig. 1.33). A firewall examines each message and blocks those the specified security criteria.