LECTURE 1

NETWORKING

1. Internet

The uses and the actual physical size of the Internet grows day-to-day. It is an area of technology that is immersed in jargon and ignorance. Many people often confuse the World Wide Web(WWW) with the Internet, but they have different purposes. The Internet, itself, is basically the global interconnection of networks and independently connected computers, whereas the WWW is a collection of computers which store digital information and, using a standard transmission method, transmit it over the Internet. The WWW is thus one of the uses of the Internet, others include:

- Electronic mail.
- The connection of remote computers.
- Video conferencing
- Remote control of remote equipment
- Remote data acquisition

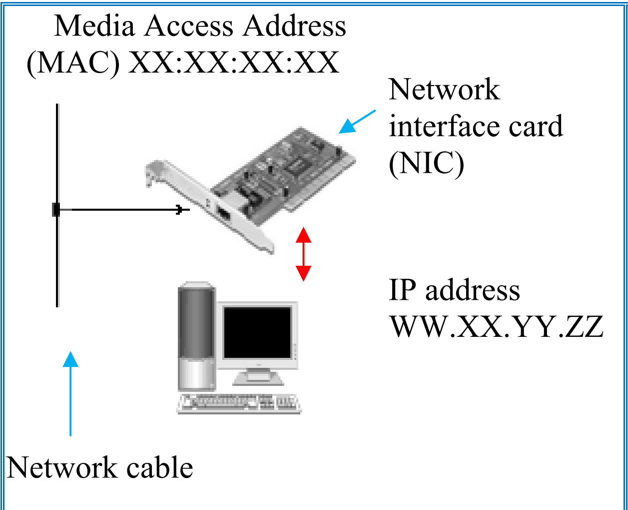
The Internet basically exists as a global network. It is not owned by any one organization or country and is thus not controlled by any political pressures. The data which is carried on the Internet is obviously governed by laws and regulations.

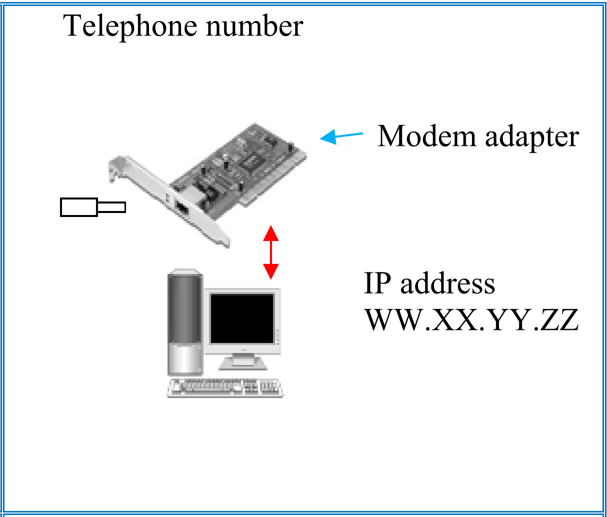
1.2. Standardized addressing

The Internet is an infrastructure of interconnected networks which communicate using the TCP/IP(Transport Control Protocol/Internet Protocol) standard. It can be viewed as a matrix of networks and independently connected computers.

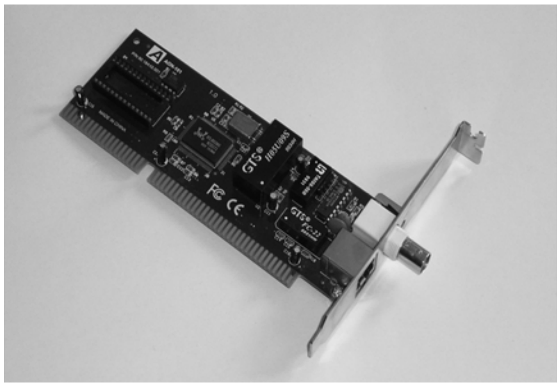
Each node on the Internet has an associated IP address, in the form of W. X.Y.Z and, if they connect to a local area network, have a unique physical address of the form XX:XX:XX:XX(normally called MAC address). If the node connects to a telephone connection then its telephone number is equivalent to the MAC address, as illustrated in Figure 1. In general, the IP address is used to route data through the Internet and the MAC address is used to send data from one node to the next.

One way to imagine the relationship between the IP address and the MAC address is to relate it to the transport of a letter through the postal service. Most letters now have a postal(or zip)code along with the full address of the destination. The postal(or zip) code is then used to quickly route the letter through the postal system. Then when it arrives at the area sorting office the actual address of the letter is used to locate the destination of the recipient.





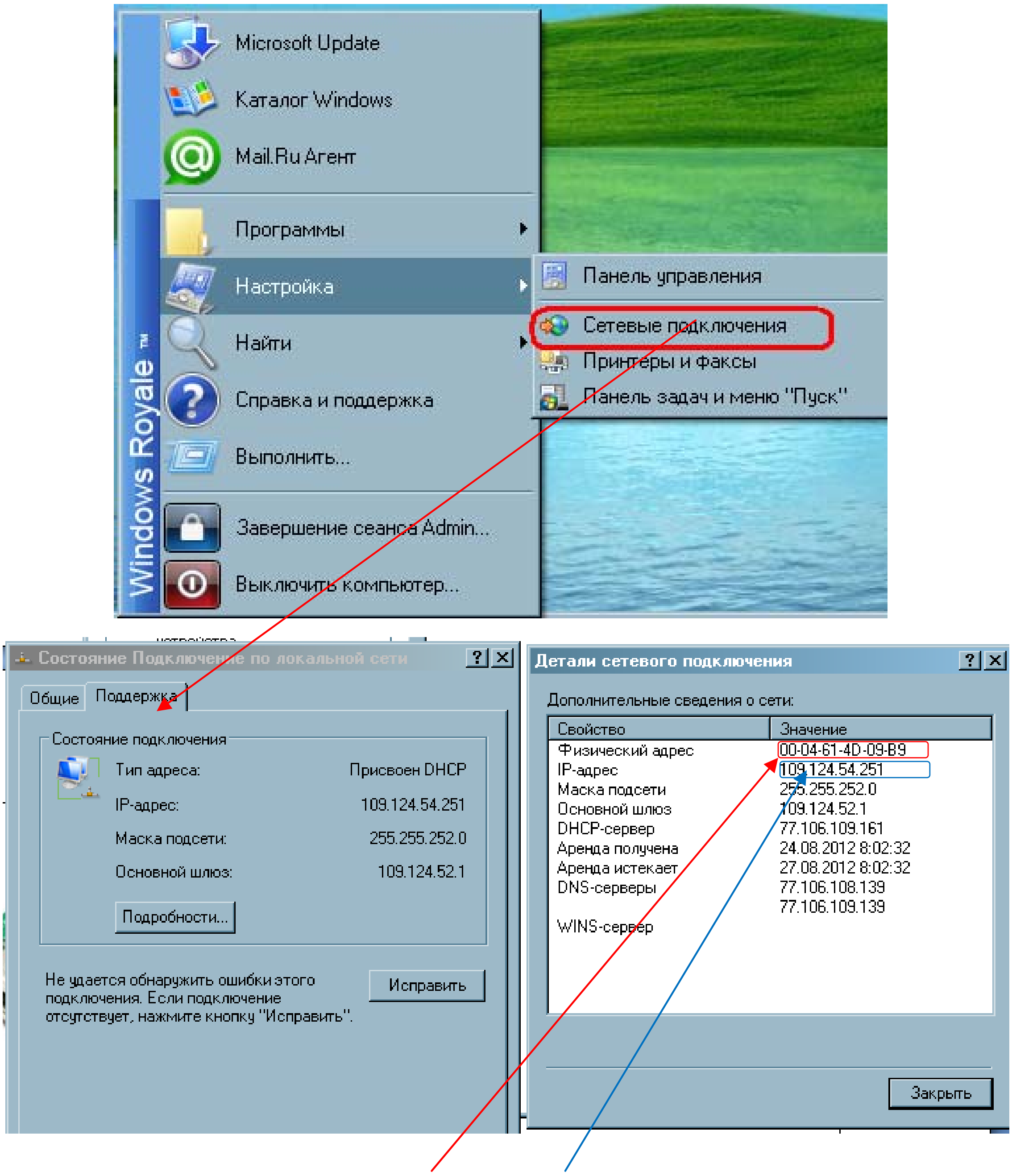
An integrated network interface card on a system.



Network interface card (NIC).

Figure 1 (Сетевая плата - сетевой адаптер)

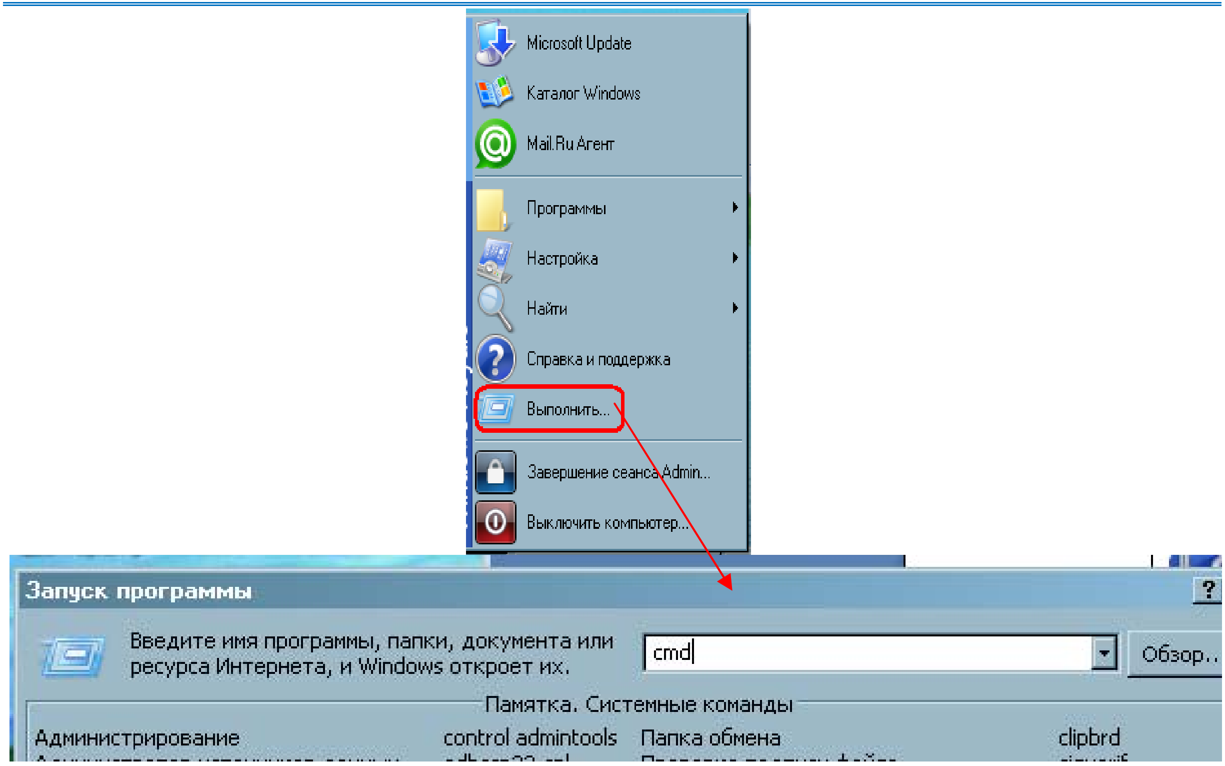
How to get IP address and MAC address on your computer (Windows NT) is illustrated in Figure 2

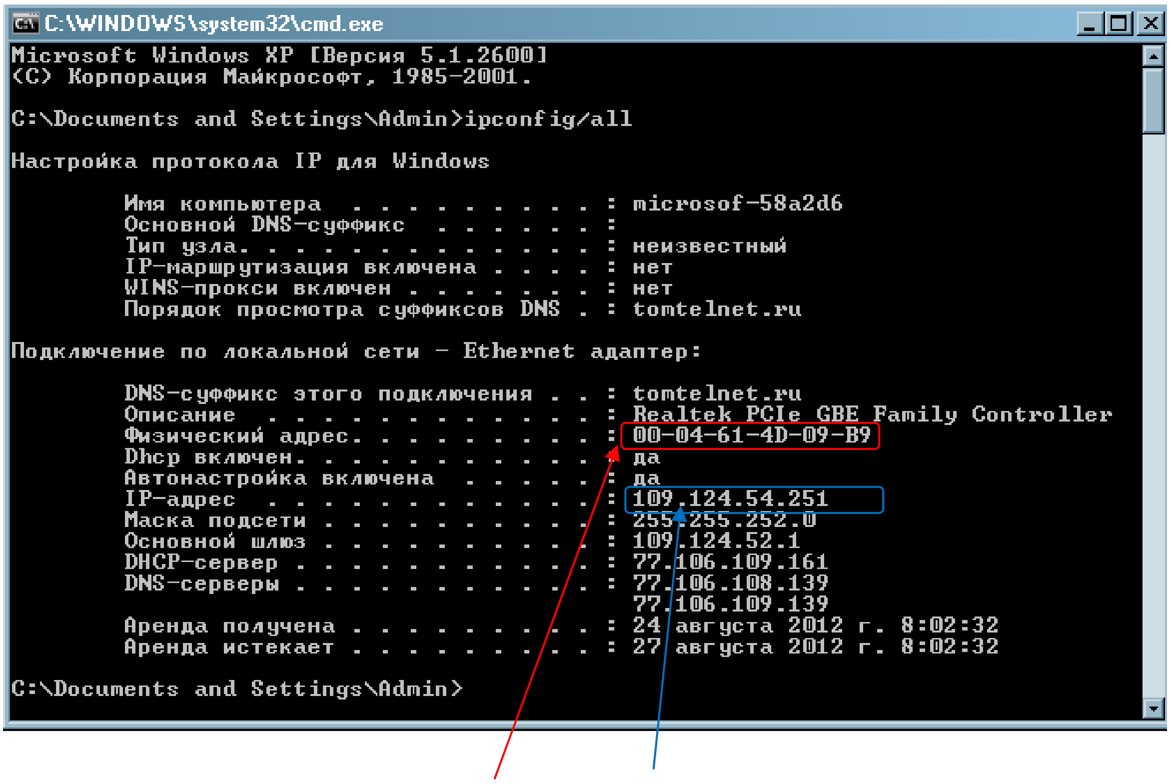


MAC address, IP address

Figure 2

Or you can get the IP address and MAC adderess using comand line. To start a command prompt, select **Start | Run**, type **CMD**, and then press Enter. When the command prompt appears, type **ipconfig /all** to view your TCP/IP settings and MAC address (is illustrated in Figure 3).





MAC address, IP address

Figure 3

1.3. LANs, WANs and MANs

Computer systems operate on digital data and can communicate with other digital equipment over a network or through an independent connection. Networks are normally defined as either:

- Wide area networks (WANs), which normally connect networks over a large physical area, such as between different buildings, towns or even countries.
- Local area networks(LANs), which connect computers within a single office or building. They typically connect to a common electronic connection – commonly known as a network backbone. LANs can connect to other networks either directly or through a WAN.
- Metropolitan area networks(MANs), which normally connect networks around a town or city. An example of a MAN is the EaStMAN network which connects universities and colleges in Edinburgh and Stirling, UK.

The four main methods of connecting a network(or an independently connected computer)to another network are:

- Through a modem connection. A modem converts digital data into and analogue form that can be transmitted over a standard telephone line.
- Through an ISDN connection. An ISDN (integrated services digital network) connection uses the public telephone service. It differs from a modem connection is that the data sent is in a digital from.
- Through a gateway. A gateway connects one type of network to another type.
- Through a bridge or router. Bridges and routers normally connect one type of network to one of the same type.

Modems are used to connect a network(or independently attached computer)over the public switched telecommunications network(PSTN). Normally telephone-type connections are unsuitable for digital data as they have a limited band width of between 400 to 3400 Hz. The modem must then be used to convert the digital information into an analogue form which is transmittable over the telephone lines. Figure 4 illustrates the connection of computers to a PSTN.

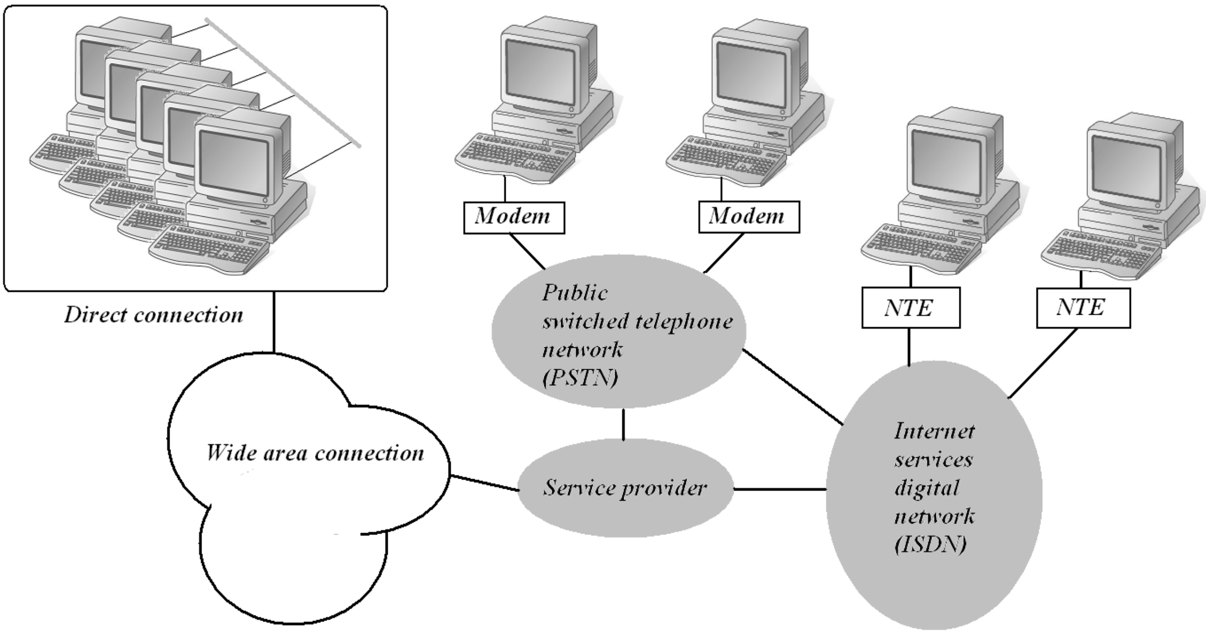


Figure 4. Connection of nodes to a PSTN

These computers can connect to the WAN through a service provider(such as CompuServe) or through another network which is connected by modem. The service provider has the required hardware to connect to the WAN.

ISDN allows the transmission of many types of digital data into a truly global digital network. Transmittable data types include digitized video, digitized speech and computer data. Since the switching and transmission are digital, fast access times and relatively high bit-rates are possible. Typical base bit rates include 64 kbps. All connections to the ISDN require network termination equipment(NTE).

1.4. OSI model

A major problem in the electronics industry is the interconnection of equipment and the compatibility of software. Other problems can occur in the connection of electronic equipment in one part of the world to another in another part. For these reasons the International Standards Organisation(ISO) developed a model known as the OSI(open systems interconnection) model. Its main objects were to:

- Allow manufacturers of different systems to interconnect their equipment through standard interfaces.
- Allow software and hardware to integrate well and be portable on differing systems.
- Create a model which all the countries of the world use.

The OSI model is shown in Figure 5. Data passes from the top layer of the sender to the bottom and then up from the bottom layer to the top of the recipient. Each layer on the transmitter, though, communicates directly the recipient's corresponding layer. This creates a virtual data flow between layers.

The top layer(the application layer) initially gets data from an application and appends it with that the recipients application layer will read. This appended data passes to the next layer(the presentation layer). Again it appends its own data, and so on, down to the physical layer. The physical layer is then responsible for transmitting the data to the recipient. The data sent can be termed a data packet or data frame.

Figure 5 below shows the basic functions of each of the layers.

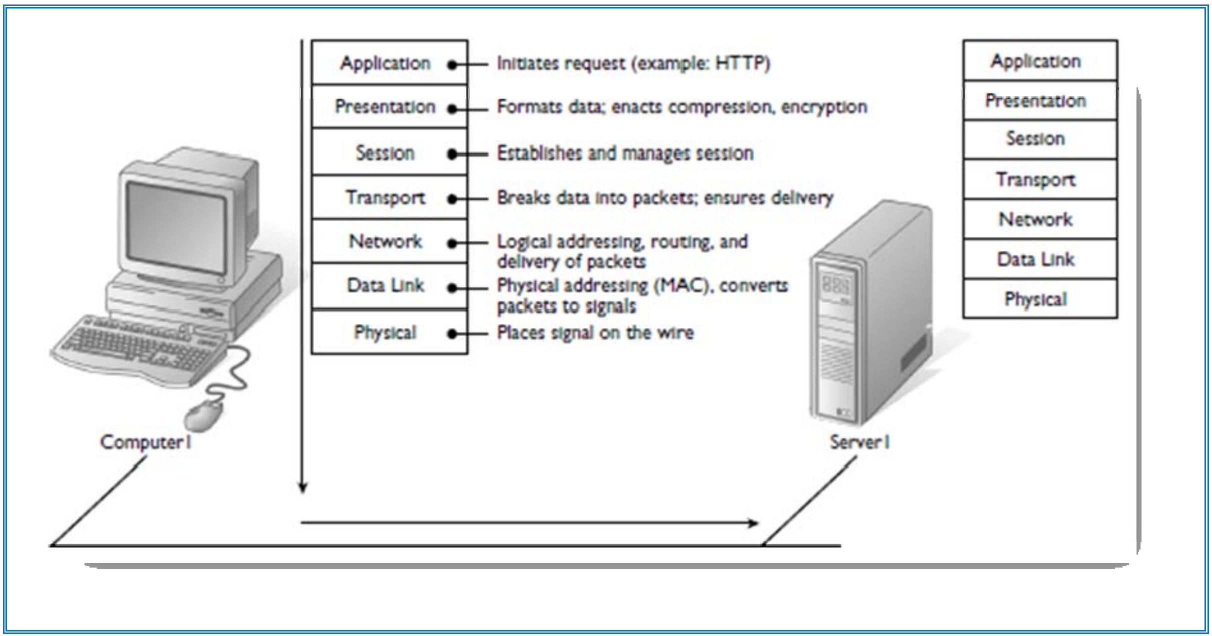


Figure 5

The functions of the layers are:

1. ***Physical***. Defines the electrical characteristics of the communications channel and transmitted signals, such as voltage levels, connector types, cabling, and so on. The bottom layer of the OSI hierarchy is concerned only with moving bits of data onto and off the network medium. The physical layer does not define what that medium is, but it must define how to access it. This includes the physical topology (or structure) of the network, the electrical and physical aspects of the medium used, and encoding and timing of bit transmission and reception. In our example, once the network layer has appended the logical addresses and passed the data to the data link layer where the MAC addresses have been appended
2. ***Data link***. Ensures that the transmitted bits are received in a reliable way, such as adding extra bits to define the start and end of a data frame, adding extra error detection/correction bits and ensuring that multiple nodes do not try to access a common communication channel at the same time. The data link layer is responsible for converting the data from a packet to a pattern of electrical bit signals that will be used to send the data across the communication medium. On the receiving system, the electrical signals will be converted to packets by the data link layer and then passed up to the network layer for further processing. The data link layer is divided into two sublayers:

    ■ *Logical link control* (LLC) is responsible for error correction and control functions.

    ■ *Media access control* (MAC) determines the physical addressing of the hosts. The MAC sublayer maintains physical device addresses (commonly referred to as *MAC addresses*) for communicating with other devices on the network. These physical addresses are burned into the network cards and constitute the low-level address used to determine the source and destination of network traffic. In our example, once the sending system's network layer appends the IP address information, the data link layer will append the MAC address information for the sending and receiving systems. This layer will also prepare the data for the wire by converting the packets to binary signals. On the receiving system, the data link layer will convert the signals passed to it by the physical layer to data and then pass the packets to the network layer for further processing.

3. ***Network***. Routes data frames through a network. If data packets require to go out of a network then the transport layer routes it through interconnected networks. Its task may involve, for example, splitting up data for transmission and re-assembling it upon reception.
4. ***Transport***. Provides an open communications path with the other system. It involves the setting up, maintaining and closing down a session. The communication channel and the internetworking of the data should be transparent to the session layer.
5. ***Session***. Provides an open communications path with the other system. It involves the setting up, maintaining and closing down of a session. The communication channel and the internetworking of the data should be transparent to the session layer.
6. ***Presentation***. Uses a set of translations that allows the data to the interpreted properly. It may have to carry out translations between two systems if they use different presentation standards such as different character sets of differing character codes . The presentation layer can also add data encryption for security purposes. After the request is made, the application layer passes the data down to the presentation layer, where it is to be formatted so that the data (or request) can be interpreted by the receiving system. When the presentation layer receives data from the application layer to be sent over the network, it makes sure that the data is in the proper format—if it is not, the presentation layer converts the data. On the receiving system, when the presentation layer receives network data from the session layer, it makes sure

that the data is in the proper format and once again converts it if it is not. Formatting functions that could occur at the presentation layer could be compression, encryption, and ensuring that the character code set can be interpreted on the other side. For example, if we choose to compress our data from the application that we are using, the application layer will pass that request to the presentation layer, but it will be the presentation layer that does the compression. Now, at some point, this data must be decompressed so that it can be read. When the data reaches the presentation layer of the receiving computer, it will decompress the data and pass the data up to the application layer.

7. ***Application.*** Provides network services to application programs such as file. The application layer running on the sending system is responsible for the actual request to be made. This could be any type of networking request—a web request using a web browser (HTTP), an email delivery request using SMTP, or a file system request using the network client redirector software.
   On the receiving system, the application layer would be responsible for passing the request to the appropriate application or service on that system.

Figure5 shows how typical networking systems fit into the OSI model. The data link and physical layers are covered by networking technologies such as Ethernet, Token Ring and FDDI. The networking layer is covered by IP(internet protocol) and transport by TCP(transport control protocol). The IP part routes data packets through interconnected networks and TCP sets up a reliable transfer mechanism between the communication nodes.

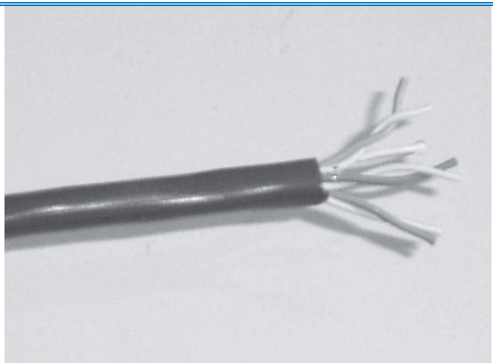
1.5. Network cable types

The cable type used on a network depends on several parameters, including:

- The data bit rate.
- The reliability of the cable and the maximum length between nodes.
- The possibility of electrical hazards and tolerance to harsh conditions.

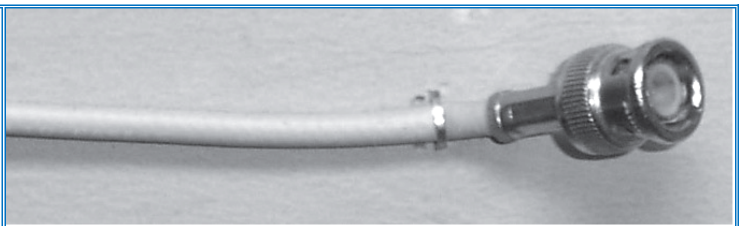
- Power loss in the cables.
- Expense and general availability of the cable.
- Ease of connection and maintenance.
- Ease of running cables, and so on.

The main types of cables used in networks are twisted-pair, coaxial and fibre optic, these are illustrated in Figure 6.


Unshielded twisted-pair (UTP) cable.


An RJ-45 connector used to connect UTP cable to a network card.

Both UTP and STP cabling have a maximum distance of 100 meters


Coaxial cable with a BNC connector.


A fiber-optic cable.

The maximum length of the fibre optic cable is 20 km

Figure 6.

Twisted –pair and coaxial cables transmit electric signals, whereas fibre optic cables transmit light pulses. Unshielded twisted-pair (UTP) cables are not shielded and thus interfere with nearby cables, whereas shielded twisted-pair cables(STP) cause less interference. Public telephone lines generally use twisted-pair cables. In LANs, they are generally used with bit rates of 10 Mbps and with maximum lengths of 100 m(although high-specification STP cables can transmit data at up to 100 Mbps). Coaxial cables have a grounded metal sheath around the signal conductor. This limits the amount of interference between cables and thus allows higher data rates. Typically, they are used at bit rates of 100 Mbps for maximum legths of 1 km.

The highest specification of the three cables is fibre optic. This type of cable allows extremely high bit rates over long distances. Fibre optic cables do not interfere with nearby cables and give greater security, give more protection from electrical damage by external equipment, are more resistant to harsh environment and are safer in hazardous environments.

A typical bit rate for a LAN using fibre optic cables is 100 Mbps, in other applications this can reach several gigabits/sec. The maximum length of the fibre optic cable depends on the transmitter and receiver electronics but a single length of 20 km is possible (Fig. 6).