Savitribai Phule Pune University

Centre for Information and Network Security

Course: Introduction to Cyber Security / Information Security

Module 1: Pre-requisites in Information and Network Security

Chapter 1: Overview of Networking Concepts

Overview of Networking Concepts

Basics of Communication Systems

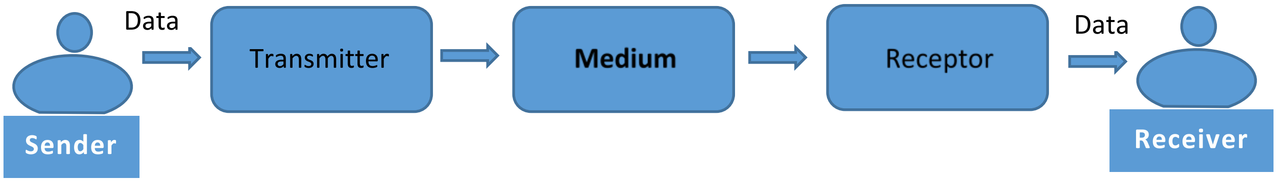
Communication has always been an integral part of human life. The dictionary meaning of 'communication' is: the activity or process of expressing ideas or feelings or of giving people information. It can be point to point that happens between only two entities like person to person or it can be point to multipoint that happens between one person to many like radio or television.

Over the period the means and ways of communication have evolved right from individual level to enterprise level. Nowadays communication systems have become backbone of today's world. Communication that happens over a long distance is called telecommunication. Radio, television, telephones are few traditional forms of telecommunication systems. With the advent of newer technologies like satellite communication and internet, telecommunication systems now are more efficient and reliable. They are capable of giving better quality of service to the users.

There are different components of communication system. It comprises of:

a. Sender (Source):
   He is the one who wants to send some message to the receiver.
b. Transmitter:
   The set of devices which converts the message in to a form that is suitable for transmission over designated medium.
c. Medium:
   Medium carries transmitted signal over a distance up to the receptor.
d. Receptor:
   It is the set of devices which catch the transmitted signal from the medium and convert it into the original message.
e. Receiver (Destination): He is the one to whom the sender wants to send message.
f. Data: The message that sender wants to send to the receiver.

The basic block diagram of communication system is as given below.



Sender who wants to send the data to receiver feeds the data to transmitter. Transmitter processes or encodes the data to generate signals which can propagate and carry the data over the medium. These signals are captured by the receptor at receiver end. Receptor decodes intercepted signals to generate original data and gives it to the receiver.

When two persons speak with each other, the sound produced by vocal chords is thrown out (transmitted) by the mouth cavity in the air. This produces sound waves in the air. The ears of another person become receptor of these waves and the meaning is interpreted by brain of that person.

In today's networked world there are varied technologies and means of telecommunication. The above diagram is the basic one and is applicable to any type of communication system. The complexity of each of the above mentioned component varies with the very purpose of the system and the end users of the system. For example, the system designed to allow long distance wireless communication of police is far different than DTH (Direct to Home) television broadcasting.

So far as communication using two computers is concerned, the system becomes more complicated.

Let us consider the example: While sitting in her home, Ms Tanvi from Pune is writing an email to Mr Umesh who is travelling in London. Both Umesh and Tanvi will need:

- Email accounts
- Internet connectivity
- User End devices: Laptop/Computer/Tab/smartphone

In this case, the computer that Tanvi is using, becomes the transmitter. Internet service providers (ISP) may use media (plural of medium) like wireless or cables or Optical Fibers to provide them internet connectivity. The email will be transferred through internet. If Umesh receives and read it using his smartphone, the smartphone becomes receptor here. This computer communication is accomplished by following special set of rules called protocols. Besides it there are few governing bodies which facilitate smooth functioning of computer communications.

In any communication system, the medium of communication decides how long the signal can be carried.

Transmission Media

In computer networks there are two types of media.

a. Wired
b. Wireless

Wired

Wired medium is a medium wherein physical connectivity is there between two nearby end points. The most common forms of wired media are:

i. Twisted Pair Cable

In pair cables generally there are four pairs of copper wires bundled together in a plastic sheath. Each pair has different colour. The two copper wire of the pair are twisted and enrolled on each other in a spiral form. This structure helps in minimising the interferences present in outer environment.

It is very common form of networking found in computer labs or small networks within the building.

These are generally called cat5/cat6 or Ethernet cables.

ii. Coaxial Cables:

It has a pair of conducting wires concentric to each other. The metal conductor is at the centre surrounded with the dielectric insulator. The circumferential outer conductor is placed on the dielectric. Braided sheath and outer jacket protects it from interferences and environments.

These cables can transfer higher frequency signals without losses upto considerably long distances than the twisted pair cables.

iii. Optical fibre:

Optical fibre cable (OFC) does not have metal conductor. It has thin glass conduits which transfers the signal in the form of light. The light rays pass through the inner glass. It has very high signal carrying capacity and hence used for high speed long distance connectivity.

Wireless:

As the name says, wireless network does not have any physical medium of communication. Electromagnetic radio frequency signals are used in such networks. The data to be carried is passed on to air using antenna and these signals are received at the destination.

Wi-Fi, Wi-Max are popular forms of wireless computer communication. Its range depends on the type and power of antenna and geography of the area. Buildings and similar obstructions attenuate the signal hampering the coverage. IEEE 802.11 standards describe various forms of such communication.

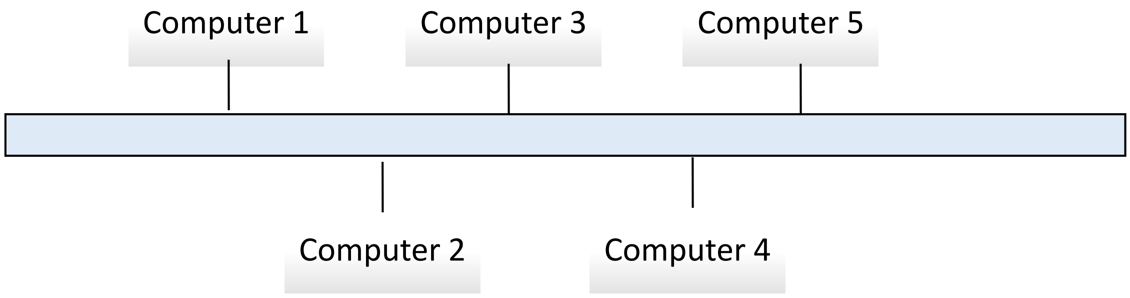
Network Topology

Network topology is the fashion in which computers (also called nodes) are connected in order to form a network.

Different topologies are

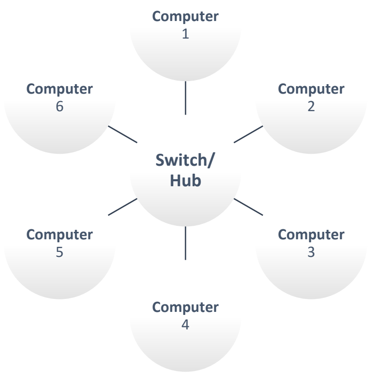
1. **Bus topology**

It is the simple topology in which computers are connected to common backbone. This common backbone is called trunk. It has terminator at one end. Only one computer can send the data in this topology.



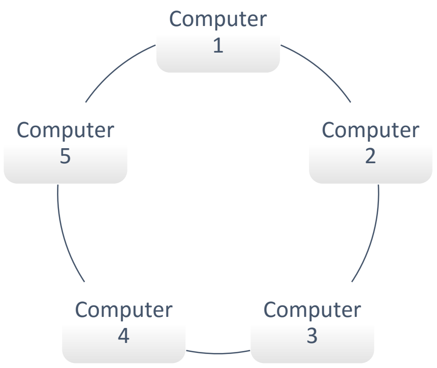
2. Star Topology

It has a central point (called hub) to which all the computers are connected. It involves more cabling. If the central unit stops functioning, entire network gets affected. More than one computer can send data in this type of topology.



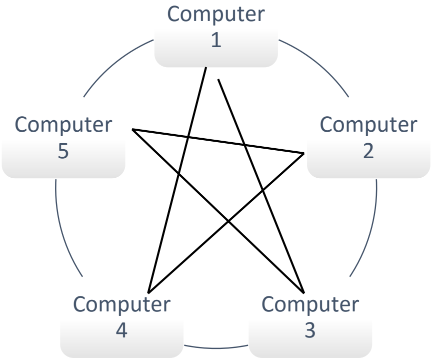
3. Ring topology

Computers are connected in ring fashion. Each computer acts as repeater and keeps passing the message over the ring. Failure of one node can affect the communication.



4. **Mesh Topology:**

Here each node is connected to all other nodes. Hence it gives better redundancy. If one segment connecting two different nodes fails, the communication can still happen through approaching the destination via different path.



5. **Hybrid Topology:**

It is mix of two or more topologies mentioned above. For example, a group of few nodes which are connected in star topology can be connected to few other nodes in a ring fashion.

Types of Networks

Computer networks can be small as in small offices having 4 to 5 computers or it can be large networks connecting thousands of computers spread over the city.

On the basis of the reach and scope, computer networks can be:

1. LAN (Local Area Network)

   Local Area Network these are smaller networks limited to a building or small group of nearby buildings or campus.
2. MAN (Metropolitan Area Network)

   These can have thousands of nodes and have a geographical spread across a big city. It may contain different smaller networks in it.
3. WAN (Wide Area Network)

   These are bigger networks containing nodes, LANs and even MANs. WAN can spread across a state or even a nation.

As the size of the network increases, the complexity in its administration and monitoring also increases.

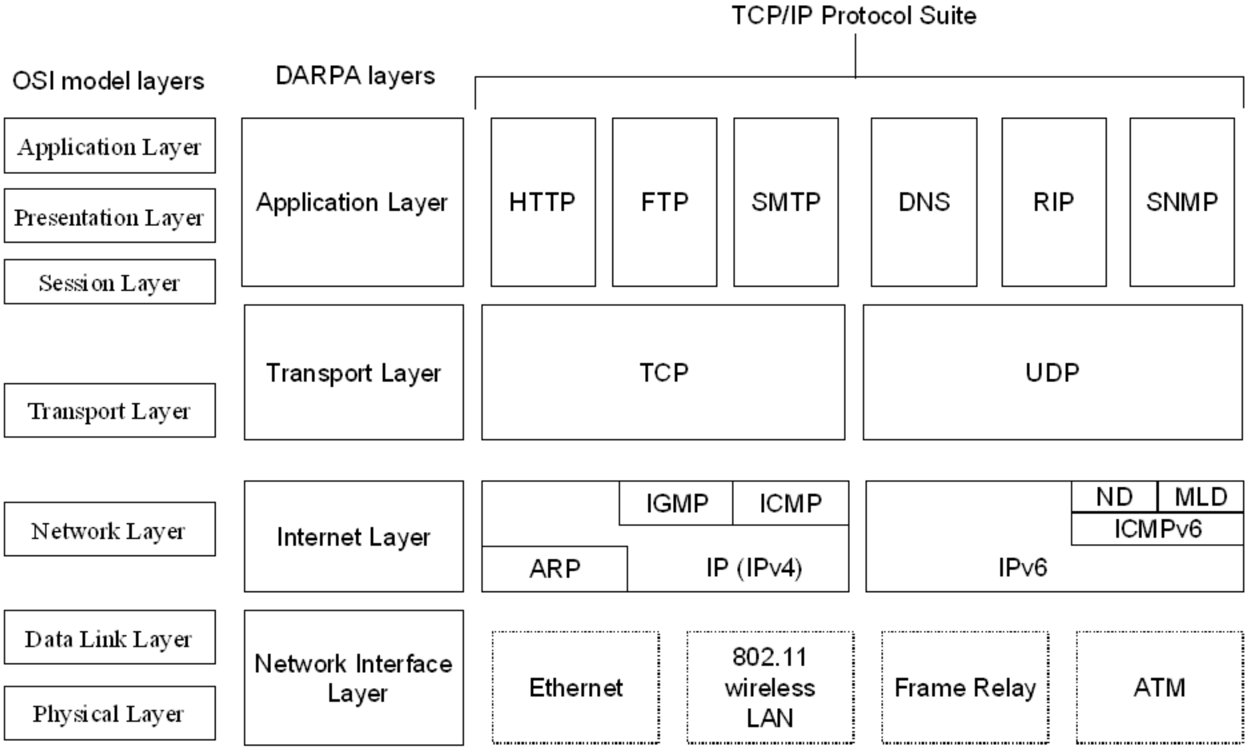
TCP/ IP protocol stack

TCP/IP stands for Transmission Control Protocol / Internet Protocol. It can almost be the synonym of today’s internet communication.

As mentioned earlier, computer connections are established and communication happens using some set of rules called protocols. All the connecting networking devices and the end user devices are supposed to adhere to these protocols for efficient communication.

TCP/IP protocol stack is the suite of networking protocols which ensures the communication is error-free, accurate and reliable one.

Figure below shows the various protocols along with the logical layers. Each of these layers has a specific role to play in the overall communication and addresses specific issues as per the roles. For example: The physical layer is concerned with the physical medium through which the communicating nodes are connected. And Data link layer ensures physical connectivity along with error checking between two adjacent nodes.



Source: https://technet.microsoft.com/en-us/library/bb726993.aspx

Wireless Networks

Wireless networks connect different nodes on the network without using any wired media. This is implemented by using radio frequency (RF) signals. The data or message to be communicated is transformed into high electric oscillations which are propagated through air in the form of electromagnetic signals.

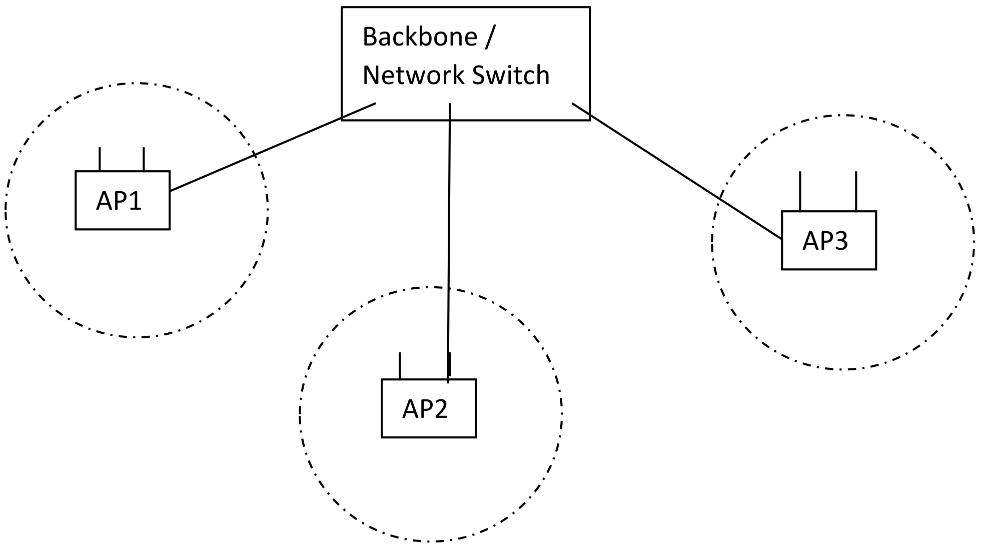
Access points (APs) are the main devices in wireless networks. AP converts the electric signal on wire into electromagnetic waves and transmits these waves into the air. Each AP zone can be identified with Service Set Identifier (SSID). SSID can also be treated as network names.

In a big wireless networks more than one APs are used. These APs are linked together through cable of another wireless signal. This linkage of APs is called backbone. Network name and the passwords are configured on the AP. In order to connect to the network, the settings on user's wireless device must match with the ones on the AP.

Wireless networks can be point-to-point (connecting two long distance points) or point-to-multipoint (connecting one point to many other points).

Wireless networks are highly scalable networks as no cabling is involved. At the same time these are more prone to security attacks as the signal on air can easily be intercepted by the attacker without physically accessing your network. For example: a wireless modem or router supplied by internet service provider (ISP) in a house may radiate the signal outside the house through windows or through walls.

IEEE802.11 set of standards explains various wireless sub-standards like IEEE802.11a, IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.11ac etc. Each of these standards have different features like speed of connectivity, operating frequency etc.



Internet

Internet is a global public network of interconnected computer networks linking billions of devices and nodes. It is called a network of networks. The interconnected networks can be private, public, educational, government or any other networks. Various protocols mentioned earlier in this chapter, few governing bodies and communities ensure efficiency and reliability of internet communication. IETF, ISOC, ICANN, IGF are few of the bodies which address the issues involved in internet.

Once connected to internet, the information available on various servers (high capacity computers which are mostly called web server on which website is hosted) on the internet can be accessed by using internet browsing tools and applications like internet explorer, Mozilla firefox, Google chrome or Apple safari.

***