Basics of Networking and Security

1 COMPUTER NETWORKS

A computer network is an interconnection of various computer systems located at different places. In computer network two or more computers are linked together with a medium and data communication devices for the purpose of communicating data and sharing resources. The computer that provides resources to other computers on a network is known as server. In the network the individual computers, which access shared network resources, are known as workstations or nodes.

Computer Networks may be classified on the basis of geographical area in three broad categories.

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)

1. Local Area Network

Networks used to interconnect computers in a single room, rooms within a building or buildings on one site are called Local Area Network (LAN). LAN transmits data with a speed of several megabits per second (106 bits per second). The transmission medium is normally coaxial cables.

LAN links computers, i.e., software and hardware, in the same area for the purpose of sharing information. Usually LAN links computers within a limited geographical area because they must be connected by a cable, which is quite expensive. People working in LAN get more capabilities in data processing, work processing and other information exchange compared to stand-alone computers. Because of this information exchange most of the business and government organisations are using LAN.

Major Characteristics of LAN

- every computer has the potential to communicate with any other computers of the network
- high degree of interconnection between computers
- easy physical connection of computers in a network
- inexpensive medium of data transmission
- high data transmission rate

Advantages

- The reliability of network is high because the failure of one computer in the network does not effect the functioning for other computers.
- Addition of new computer to network is easy.
- High rate of data transmission is possible.
- Peripheral devices like magnetic disk and printer can be shared by other computers.

Disadvantages

If the communication line fails, the entire network system breaks down.

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India

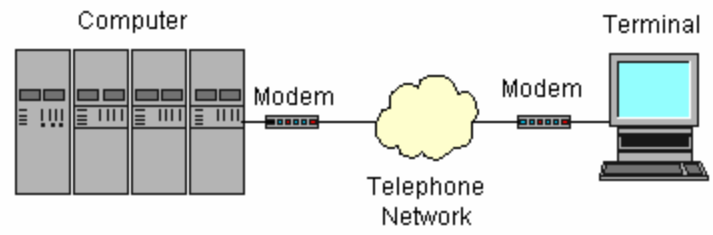
Use of LAN
Followings are the major areas where LAN is normally used:

? File transfers and Access
? Word and text processing
? Electronic message handling
? Remote database access
? Personal computing
? Digital voice transmission and storage

2. Metropolitan Area Network

Networks used to interconnect computers in a city or a town are called Metropolitan Area Networks. Generally telephone lines are used to connect these computers. Alternatively, wireless mode also is used for this purpose. Computers are connected to the telephone lines through devices called MODEMS.

Modems
The word modem is a contraction of the words modulator-demodulator. A modem is typically used to send digital data over a phone line. The sending modem modulates the data into a signal that is compatible with the phone line, and the receiving modem demodulates the signal back into digital data. Wireless modems are also frequently seen converting data into radio signals and back.



3. Wide Area Network

The term Wide Area Network (WAN) is used to describe a computer network spanning a regional, national or global area. For example, for a large company the head quarters might be at Delhi and regional branches at Bombay, Madras, Bangalore and Calcutta. Here regional centers are connected to head quarters through WAN. The distance between computers connected to WAN is larger. Therefore the transmission medium used are normally telephone lines, microwaves and satellite links.

Characteristics of WAN
Followings are the major characteristics of WAN.

1. Communication Facility: For a big company spanning over different parts of the country the employees can save long distance phone calls and it overcomes the time lag in overseas

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India

communications. Computer conferencing is another use of WAN where users communicate with each other through their computer system.

2. Remote Data Entry: Remote data entry is possible in WAN. It means sitting at any location you can enter data, update data and query other information of any computer attached to the WAN but located in other cities. For example, suppose you are sitting at Madras and want to see some data of a computer located at Delhi, you can do it through WAN.

3. Centralised Information: In modern computerised environment you will find that big organisations go for centralised data storage. This means if the organisation is spread over many cities, they keep their important business data in a single place. As the data are generated at different sites, WAN permits collection of this data from different sites and save at a single site.

Difference between LAN and WAN

? LAN is restricted to limited geographical area of few kilometers. But WAN covers great distance and operate nationwide or even worldwide.

? In LAN, the computer terminals and peripheral devices are connected with wires and coaxial cables. In WAN there is no physical connection. Communication is done through telephone lines and satellite links.

? Cost of data transmission in LAN is less because the transmission medium is owned by a single organisation. In case of WAN the cost of data transmission is very high because the transmission medium used are hired, either telephone lines or satellite links.

? The speed of data transmission is much higher in LAN than in WAN. The transmission speed in LAN varies from 0.1 to 100 megabits per second. In case of WAN the speed ranges from 1800 to 9600 bits per second (bps).

? Few data transmission errors occur in LAN compared to WAN. It is because in LAN the distance covered is negligible.

NETWORK TOPOLOGY

The term topology in the context of communication network refers to the way the computers or workstations in the network are linked together. According to the physical arrangements of workstations and nature of work, there are three major types of network topology. They are star topology, bus topology and ring topology.

Star topology

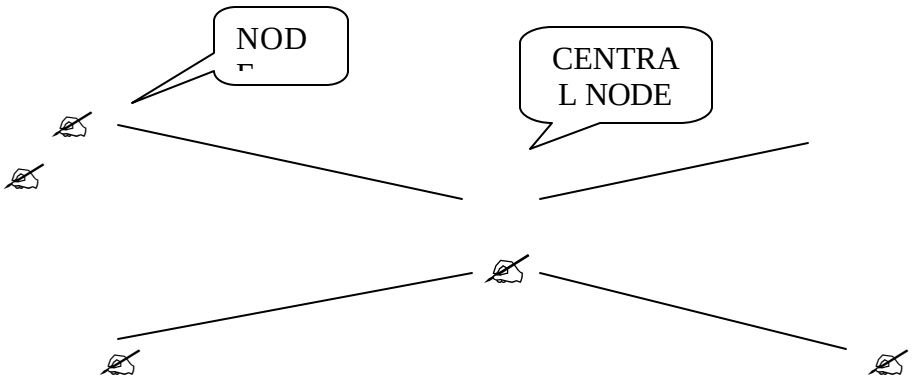
In star topology a number of workstations (or nodes) are directly linked to a central node (see, Fig. 4.3). Any communication between stations on a star LAN must pass through the central node. There is bi-directional communication between various nodes. The central node controls all the activities of the nodes. The advantages of the star topology are:

? It offers flexibility of adding or deleting of workstations from the network.

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India

? Breakdown of one station does not affect any other device on the network.

The major disadvantage of star topology is that failure of the central node disables communication throughout the whole network.



Star Topology

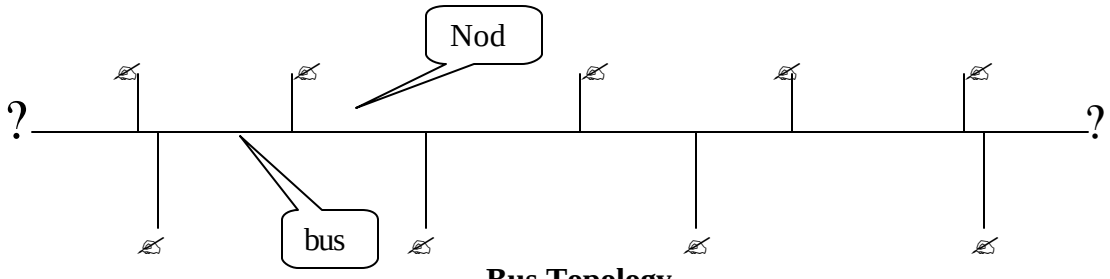
Bus Topology

In bus topology all workstations are connected to a single communication line called bus. In this type of network topology there is no central node as in star topology. Transmission from any station travels the length of the bus in both directions and can be received by all workstations. The advantage of the bus topology is that

? It is quite easy to set up.

? If one station of the topology fails it does not affect the entire system.

The disadvantage of bus topology is that any break in the bus is difficult to identify.



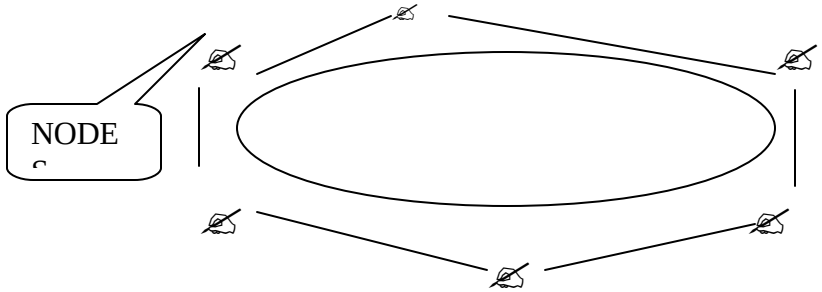
Bus Topology

Ring Topology

In ring topology each station is attached nearby stations on a point to point basis so that the entire system is in the form of a ring. In this topology data is transmitted in one direction only. Thus the data packets circulate along the ring in either clockwise or anti-clockwise direction. The advantage of this topology is that any signal transmitted on the network passes through all the

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India

LAN stations. The disadvantage of ring network is that the breakdown of any one station on the ring can disable the entire system.



Ring Topology

Communication Devices

Following are the major communication devices used today

Wire Pairs:

Wire pairs are commonly used in local telephone communication and for short distance digital data communication. They are usually made up of copper and the pair of wires is twisted together. Data transmission speed is normally 9600 bits per second in a distance of 100 meter.

Coaxial Cables:

Coaxial cable is groups of specially wrapped and insulted wires that are able to transfer data at higher rate. They consist of a central copper wire surrounded by an insulation over which copper mesh is placed. They are used for long distance telephone lines and local area network for their noise immunity and faster data transfer.

Microwave:

Microwave system uses very high frequency radio signals to transmit data through space. The transmitter and receiver of a microwave system should be in line-of-sight because the radio signal cannot bend. With microwave very long distance transmission is not possible. In order to overcome the problem of line of sight and power amplification of weak signal, repeaters are used at intervals of 25 to 30 kilometers between the transmitting and receiving end.

Communication Satellite:

The problem of line-sight and repeaters are overcome by using satellites, which are the most widely used data transmission media in modern days. A communication satellite is a microwave relay station placed in outer space. INSAT-1B is such a satellite that can be accessible from anywhere in India. In satellite communication, microwave signal is transmitted from a transmitter on earth to the satellite at space. The satellite amplifies the weak signal and transmits it back to the receiver. The main advantage of satellite communication is that it is a single microwave relay station visible from any point of a very large area. In microwave the data transmission rate is 16 Giga bits per second. They are mostly used to link big metropolitan cities.

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India

Information Security

What is information security?

Information security is characterized as the preservation of:

- **Confidentiality** – ensuring that information is accessible only to those authorized to have access.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods
- **Availability** – ensuring that authorized users have access to information and relating assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational practices and software functions

Why information security?

Information systems are prone to potential expensive security risk and threats leading to high client concerns for IPR (Intellectual property rights) protection. According to the "2000 Information Security Industry Survey" published by ICSA (International Computer Security Association), the top 3 IT security concerns are

- Malicious Code (includes viruses, Trojans, worms, and hostile ActiveX and Java)
- Loss of Privacy/Confidentiality (includes abuse/misuse of data) and
- Electronic Exploits/Tools (includes cracking, eavesdropping, spoofing and toolkits).

If information assets are not suitable protected, it can be

- Given away or stolen without depriving you of it.
- Modified without your knowledge to make it worthless.
- List without trace or hope of recovery
- Violation of IPR leading to lawsuits / loss of customer confidence.
- Corruption / loss of integrity of importance date e.g. software codes
- Loss of business due to leakage / theft of company intellectual property
- Mobile workforce not able to access internal IT systems
- Unanticipated disruption in off-site work due to break down of communication links.
- Leak and unauthorized use of confidential information, business strategy.
- Physical damages / theft of critical IT infrastructure component.

Information security through network access control

What is Network access control?

- Imposition of certain controls to restrict access to a shared network based on the access control policy.
- The controls can be implemented by putting firewall at the network perimeter.
- The firewall filters traffic by means of predefined tables or set of rules.

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India

Firewall

Firewall is an intermediate system plugged between two networks, which can act as a security wall. The main purpose of a firewall is to control access to or from a protected/trusted network. It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

Without firewall a site is more exposed to inherently insecure host operating systems, TCP/IP vulnerabilities and attacks from the Internet. It is also very difficult to maintain same level of security for all the hosts in a network.

Benefits of firewall

- Protection from vulnerable services e.g. NIS, NFS, source routed packets
- Controlled access
  - Help to control access to and from a network.
- Concentrated security
  - Additional security measures e.g. one time password system etc. can be implemented in single place at the firewall instead of in individual host.
- Enhanced privacy
  - Blocking of services like finger, DNS helps to hide information, which could otherwise be useful to the attackers.
- Logging and statistics of network use and misuse
  - Help to monitor usage of network services and detection of potential intrusion.
- Policy enforcement
  - Helps to implement organization network access control policy.

Firewall components

There are three basic components of firewall

- Firewall Policy
- Packet filters
- Application gateways

Firewall policy

The policy directly influences the design, installation and use of firewall system. The higher-level policy addresses the services that will be allowed or explicitly denied from / to the restricted network (including exception). The lower level policy describes how the firewall will actually go about restricting the access and filtering the services that are defined in the higher-level policy.

Packet filter or packet filtering Gateways

Packet filters uses routers with packet filtering rules to grant or deny access based on source IP address, destination IP address, source port and Destination port information of an IP packet. Adding TCP or UDP port filtering to IP address filtering results in great deal of flexibility. In general the packet filters operates on the each packet in individual and hence stateless but Stateful packet filters use some of the state information derived from the past communication. It can be applied on outbound interface as well as on inbound interface. When IP packets arrive at a network interface of a packet filter and are examined against the rule of filtering. Selection

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India

criteria uses information found in packet header and related to the network interfaces, the packets appear.

Application Gateway

Gateways interconnect one network to another for a specific application. Its major function is application specific and used as proxy. If an application Gateway contains proxies for FTP and TELNET, then only that traffic will be allowed and other services are completely blocked. Packet filter and application gateways are usually combined in a firewall configuration to implement the firewall policy.

Dual – homed Firewall

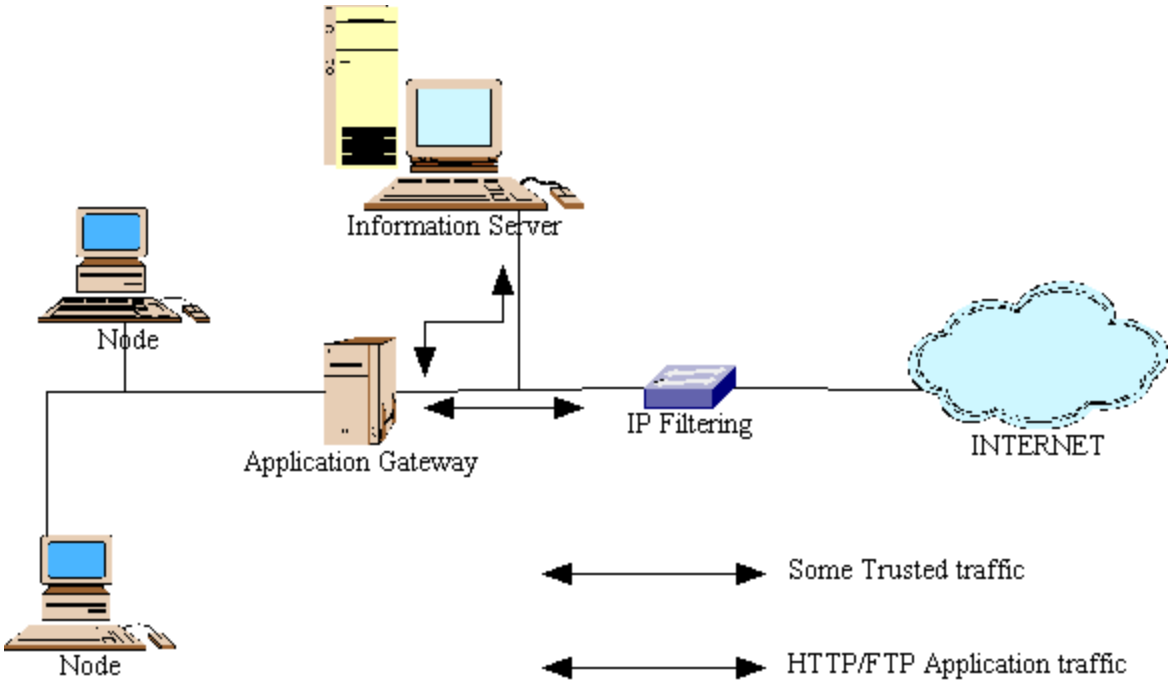


Fig: Dual-homed Firewall configuration

It is a host with two network cards, one connected to the external or untrusted network and other is to the internal or trusted network. The key security principle is not to allow traffic coming in from an untrusted network to be directed routed to the trusted network. IP source routing and IP forwarding services are disabled in this host.

© **INFLIBNET** Centre, University Grants Commission, Ahmedabad-380009, India