

3

TOPOLOGIES AND TRANSMISSION MEDIA

INTRODUCTION

The pattern of interconnection of nodes in a network is called the topology. Formally, topology can be defined as the geometric arrangement of workstations and the links among them. Topologies are designed to create order out of the potential chaos of randomly arranged workstations. The issue where do you locate a workstation in relation to the network? At the end of a branch attached to the cable? At a junction point common to two or more cables? At the end of the cable? All of the above?

There are three connection possibilities:

1. Point-to-point joins two, and only two, adjacent workstations without passing through an intermediary workstation.
2. Multipoint is a single cable shared by more than two work-stations.
3. Logical implies that workstations are able to communicate, whether or not a direct physical connection actually exists between them.

The workstations in a local area network communicate based on some combination of physical (point-to-point or multipoint) and logical connection.

Given the location of workstations and peripherals, the goal of topology is to find the most economical and efficient way to connect all users to the network resources while providing adequate capacity to handle user demands, maintain system reliability and minimise delay. The number of parameters and variables that bear on the solution is huge. Rapid change in user demands complicates the problem further.

Control of the network also affects topology. Control and topology are so

intertwined that topology often is defined as the means of implementing the control protocol. The two facets of control are access — which workstations send messages and when, and allocation — how long the workstation has access and, where broadband media are in use, how much of the channel may be used.

Control may be centralised, in which access to the network and allocation of channel is determined by one node. Intelligence also may be concentrated in the central node with the attached workstations serving primarily as terminals. Or it may be distributed, in which caseworkstations can access the network channels independently, according to a shared set of protocols. The intelligence of the network is distributed throughout the connected workstations.

The selection of a topology for a network cannot be done in isolation as it affects the choice of media and the access method used. Because it determines the strategy used in wiring a building for a LAN, it may represent the greatest single cost to be faced, and accordingly deserves some study. There are a number of factors to consider in making this choice, the most important of which are set out below (see Table 3.1).

TABLE 3.1 : Topology Comparison

Feature	BUS	Ring	Dual Ring	Star
Reliability	* High	Low	Mod	Log
Complexity	Mod	Low	Mod	* Low
Flexibility	* High	Mod	Mod	Low
Expandibility	* High	Mod	Mod	Low
Cost	* Low	Mod	High	M-High

1. **Cost** - Whatever transmission medium is chosen for a LAN, it has to be physically installed in the building. This may be a lengthy process involving the installation of cable ducts and raceways. Ideally, it is carried out before the building is occupied and should be able to accommodate foreseen growth requirements. For a network to be cost-effective, one would strive to minimise installation cost. This may be achieved by using well-understood media and also, to a lesser extent, by minimising the distances involved.
2. **Flexibility** - One of the main benefits of a LAN is the ability to have the data processing and peripheral nodes distributed around a given area. This means that computing power and equipment can be located close to the ultimate user. Because the arrangement of furniture, internal walls, etc. in offices is often subject to change, the topology should allow for easy reconfiguration of the network. This involves moving existing nodes and adding new ones.
3. **Reliability** - Failure in a LAN can take two forms. Firstly, an individual node can malfunction. This is not nearly as serious as the second type of fault where the network itself fails to operate. In the second case, although the individual nodes can function, any software making use of the facilities of the LAN will be rendered useless. The topology chosen for the network can help by detecting the location of the fault and providing some means of isolating it.

LAN TOPOLOGIES

Many topologies have been developed to cope with communication over a limited geographical area, but three major ones have influenced LAN design and implementation. Three topologies are commonly used for microcomputer local area networks. Table 3.2 gives the classification of LAN by topology. These are:

TABLE 3.2 : A LAN Classification matrix

	topology	Feature access protocol	data rate
<i>Standard LAN</i>			
Ethernet	bus (tree)	CSMA/CD	10 Mbits/sec
token bus	bus	token passing	1, 5 or 10 Mbits/sec
token ring	ring	token passing	1 or 4 Mbits/sec
Cambridge Ring	ring	empty slot	10 Mbits/sec
<i>Non-standard LAN</i>			
PABX	star	(not applicable)	(various)
micronet	bus or ring	(various)	typically < 1 Mbits/sec

1. the star or radial topology (example: PABX);
2. the bus (example: CSMA/CD, Token Bus);
3. the ring or loop (example: Token Ring, Slotted Ring).

There are also a number of hybrid network topologies which combine features of the above. Mesh topology, common in long-haul and complex mainframe networks, currently is not used by microcomputer LANs.

Bus networks are multipoint: workstations are connected to the single central communication link by individual secondary lines. Ring and Star networks use a point-to-point topology: each physical segment of cable connects two, and only two, workstations without passing through an intermediate workstation. All three are considered structured topologies.

Combinations of topologies not only are possible, but also they are becoming increasingly popular, particularly star-wired rings. The three basic LAN topologies and the major variations or hybrids will be discussed below.

TOPOLOGY EVALUATION FACTORS

Topology is of most interest as it affects LAN use in your installation. To help you select the "best" topology for your situation, a checklist of evaluation factors follows the technical definitions of each topology. Points covered include the following:

1. Application: in what size installation is the topology most appropriate?

2. Complexity: how technically complex is the topology? This factor affects installation and maintenance of the cabling.
3. Performance: how much of a traffic load can the system support?
4. System overhead: what is the comparative price fore excess capability?
5. Vulnerability: how susceptible is the topology to failure? to damage?
6. Expandability: when you are ready to extend the LAN, how easily can the topology accommodate additional workstations and cover larger distances?

Importance of the various factors is relative, not absolute, when selecting a specific LAN being maximum affected by your requirements.

STAR OR RADIAL TOPOLOGY

In a star configuration (see Figure 3.1a), each workstation is connected to a central server through a dedicated point-to-point channel. Messages are passed from a workstation to the server.

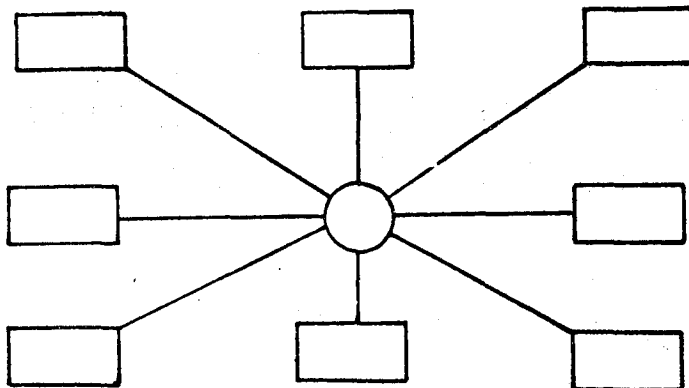


Fig. 3.1 a : The star topology

Control of the network may be allowed in one of three ways:

1. Control resides in the central server which performs all routing of messages. Data received by the central workstation may either be processed internally or forwarded for processing. In this case, the server normally provides the main computing power.
2. Control may be exercised by an outlying workstation rather than the central device. The server operates as a switch, establishing connections between workstations.
3. Control may be distributed equally to all workstations. The server is used to route messages to their destinations and to resolve conflicting requests for connections between workstations.

In all three cases the central server is the critical node: if it fails, the whole network stops.

The server provides a logical location for directly attaching the major shared resources. Generally, individual workstations do not have to make routing decisions, as all communication must pass through the central workstation before going to their destinations. **Compound star networks** (see Figure 3.2) are those in which a workstation on one network may act as server and/or controller for a secondary network. The term **snowflake** is used sometimes to refer to a compound star.

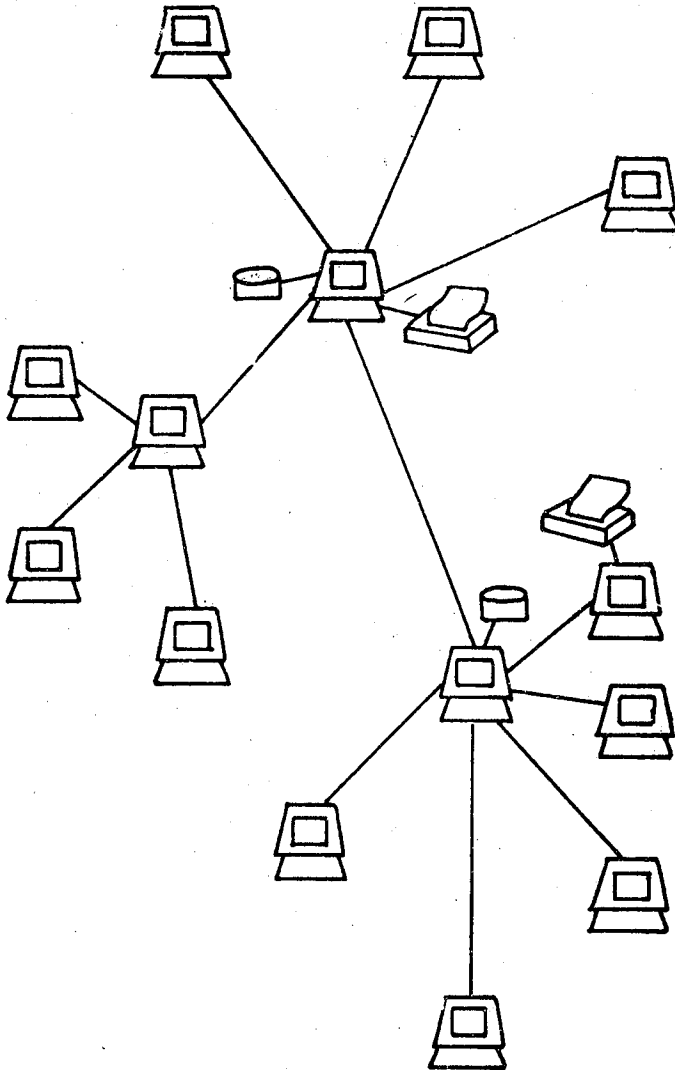


Fig. 3.2 : Compound Star or Snowflake

The size and capacity of the network is a direct function of the power of the central workstation, with the burden of compatibility placed on the central server.

Workstations do not compete for local capacity: heavy demand by one workstation does not necessarily cause a delay in network response time.

The star topology eliminates the need for each workstation on the network to make routing decisions. All message routing is localised in the central server.

Conceptually, a star is compatible with basic telephone services and is often implemented on the same lines through use of a data PBX.

This topology consists of a central node to which all other nodes are connected by a single path (see Figure 3.1a). It is the topology used in most existing information networks involving data processing or voice communication. The most common example of this is in IBM 370 installations. In this case, multiple 3270 terminals are connected to either a host computer system or a terminal controller. The connection is achieved via a single length of coaxial cable per terminal. Another example is the office PABX. In this case, each telephone is connected to a central PABX by a single dedicated voice grade twisted pair cable.

In many cases, when a building is wired with a star network, feeder cables radiate out from the centre to intermediate concentration points called **wiring closets** (see Figure 3.1b). This allows sufficient connection points to be provided for one subarea (e.g. a floor of an office building), while providing flexibility in their allocation within that area.

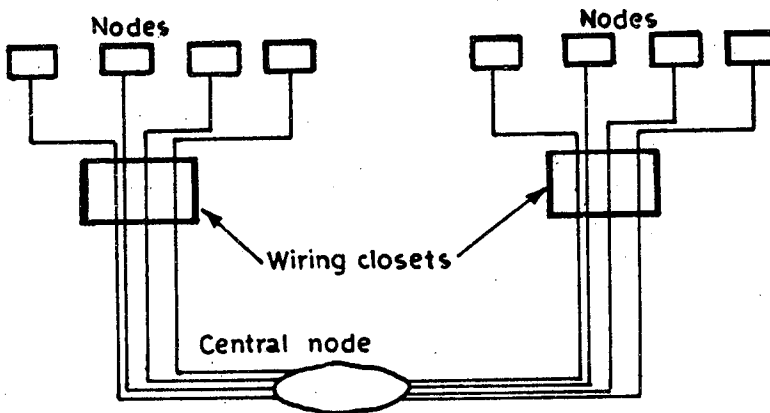


Fig. 3.1 b : The star topology using wiring closets

The two examples cited above would not qualify as LANs because in both cases, a central intelligent node is controlling the operation of all of the others. The pure star topology is seldom used in LANs, but is worthy of study because of its prevalence in more traditional data networks and its influence on the star-ring topology which is covered later.

Advantages of the Star

1. Ease of service: The star topology has a number of concentration points, i.e.

- at the central node or at intermediate wiring closets. These provide easy access for service or reconfiguration of the network.
2. **One device per connection:** Connection points in any network are inherently prone to failure. In the star topology, failure of a single connection typically involves disconnecting one node from an otherwise fully functional network.
 3. **Centralised control/problem diagnosis:** The fact that the central node is connected directly to every other node in the network means that faults are easily detected and isolated. It is a simple matter to disconnect failing nodes from the system.
 4. **Simple access protocols:** Any given connection in a star network involves only the central node and one peripheral node. In this situation, contention for who has control of the medium for transmission purposes is easily solved. Thus in a star network, access protocols are very simple.

Disadvantages of the Star

1. **Long cable length:** Because each node is directly connected to the centre, the star topology necessitates a large quantity of cable. While the cost of the cable is often small, congestion in cable ducts and maintenance and installation problems can increase costs considerably.
2. **Difficult to expand:** The addition of a new node to a star network involves a connection all the way to the central node. Expansion is usually catered for by providing large numbers of redundant cables during the initial wiring. However, problems can arise if a longer cable length is needed or an unanticipated concentration of nodes is required.
3. **Central node dependency:** If the central node in a star network fails, the entire network is rendered inoperable. This introduces heavy reliability and redundancy constraints on this node.

The star topology has found extensive application in areas where intelligence in the network is concentrated at the central node. The tendency in recent computer systems is away from host-based computing power, and the advent of microprocessor-based systems where all nodes possess a high level of processing power has led to a fall off in the use of this topology. Nevertheless, the technology is well understood and, because it is currently the dominant configuration in traditional data communication, it is likely to be with us for many years to come.

Star Evaluation Factors

- **Application:** Presently, a star network is the best way to integrate voice and data services. A star-based data network using the newer digital PBXs often can be justified by the savings and features for voice-based telephone services alone.
- **Complexity:** The star can be quite complex: workstations attached to the central workstation may in turn act as the central server for other workstations or may

be connected to communication links.

- **Performance:** Good for moderate load. However, the size and capacity of the network and hence the performance, is a direct function of the power of the central node.
- **System overhead :** Network overhead is high: the server usually cannot be used for any other purpose while acting as network server. The number of separate lines is also high.
- **Vulnerability:** System reliability is dependent on central server. If the server fails, all activity on the network ceases. Failure of an individual workstation does not affect the system. In either case, identification of problems and repair is simplified by centralised control.
- **Expandability:** Expandability may be severely restricted; most servers can support a limited number of network interfaces. Bandwidth and data rate limitations are often imposed on each user. The limits are necessary to protect the central processing functions from overload due to the aggregate rate of all the service ports and to keep the cost of each port on the central server low.

BUS TOPOLOGY

Another popular topology for data networks is the bus. This consists of a single length of the transmission medium (see Figure 3.3). This topology is used in traditional data communication networks where the host at one end of the bus communicates with several terminals attached along its length. This configuration is known as a multidrop line. It is also the topology used in the Ethernet LAN.

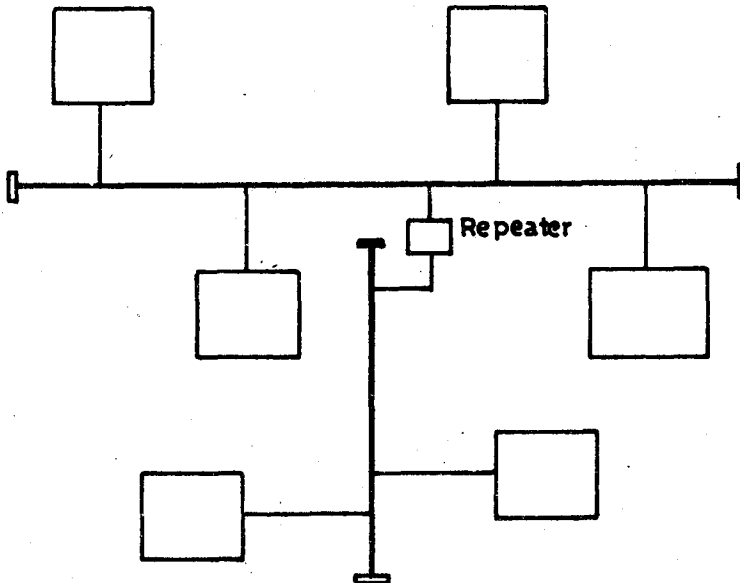


Fig. 3.3 : The bus topology

In a bus configuration, all workstations are connected to a single shared communication link through interface units and cable taps, as shown in Figure 3.3. Messages are broadcast along the whole bus. In order to receive a transmission, the workstations must be able to recognise their own address. Devices attached to a bus therefore must possess a high degree of intelligence or have the required intelligence provided by the bus interface unit.

The transmitters and receivers used by the network must tolerate a wide range of signal levels because workstations closest to the sending workstation receive a stronger signal than workstations at the far end of the bus. Signal-strength problems commonly are handled by limiting the length of the cable segments and the number of attached workstations. On some networks, amplifiers or repeaters may be used to maintain strength and clarity of the signal. Bus taps must be designed so as not to greatly reduce the signals reaching the other taps.

Advantages of the Bus

1. **Short cable length and simple wiring layout:** Because there is a single common data path connecting all nodes, the bus topology allows a very short cable length to be used. This decreases the installation cost, and also leads to a simple, easy to maintain, wiring layout.
2. **Resilient architecture:** The bus architecture has an inherent simplicity that makes it very reliable from a hardware point of view. There is a single cable through which all data passes and to which all nodes are connected.
3. **Easy to extend:** Additional nodes can be connected to an existing bus network at any point along its length. More extensive additions can be achieved by adding extra segments connected by a type of signal amplifier known as a repeater.

Disadvantages of the Bus

1. **Fault diagnosis is difficult:** Although the simplicity of the bus topology means that there is very little that can go wrong, fault detection is not a simple matter. In most LANs based on a bus, control of the network is not centralised in any particular node. This means that detection of a fault may have to be performed from many points in the network.
2. **Fault isolation is difficult:** In the star topology, a defective node can easily be isolated from the network by removing its connection at the centre. If a node is faulty on a bus, it must be rectified at the point where the node is connected to the network. Once the fault has been located, the node can simply be removed. In the case where the fault is in the network medium itself, an entire segment of the bus must be disconnected.
3. **Repeater configuration:** When a bus-type network has its backbone extended using repeaters, reconfiguration may be necessary. This may involve tailoring cable lengths, adjusting terminators, etc.
4. **Nodes must be intelligent:** Each node on the network is directly connected to

the central bus. This means that some way of deciding who can use the network at any given time must be performed in each node. It tends to increase the cost of the nodes irrespective of whether this is performed in hardware or software.

Bus Evaluation Factors

- **Application:** Bus networks are a good choice for small networks and networks with low traffic.
- **Complexity:** Bus networks tend to be relatively uncomplex.
- **Performance:** Excellent under light load, may degrade rapidly as load increases.
- **System overhead:** Comparatively low, particularly because much of the hardware is fully developed and readily available. Some redundancy of communication channel is advisable to reduce the vulnerability to channel outage.
- **Vulnerability:** Failure of one workstation on a bus network does not usually affect the network. Bus networks are vulnerable to failure from damage to the main link and other problems affecting the bus. Problems on the bus are hard to locate. Once located, however, problems are easy to repair.
- **Expandability:** Expansion and reconfiguration of a bus network are easy. A new or relocated device may be connected to the nearest convenient network access point with little disruption of the network. Interconnecting microcomputers and equipment from different manufacturers is difficult because all connected devices must be able to accept the same forms of address and data.

RING TOPOLOGY

In the case of ring or loop topology, each node is connected to two and only two neighbouring nodes. Data is accepted from one of the neighbouring nodes and is transmitted onwards to another (see Figure 3.4). Thus data travels in one direction only, from node to node around the ring. After passing through each node, it returns to the sending node, which removes it.

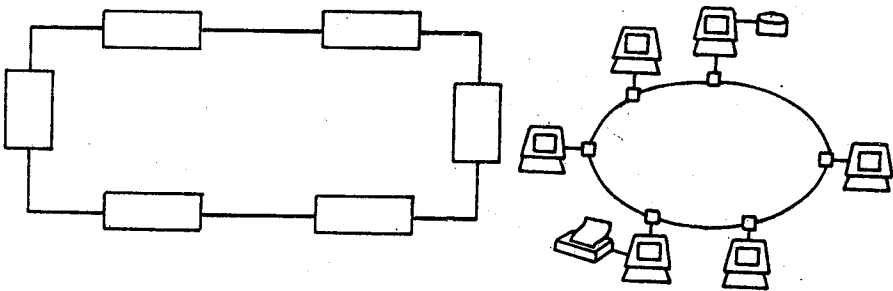


Fig. 3.4 : The ring topology

It is important to note that data 'passes through' rather than 'travels past' each node. This means that the signal may be amplified before being 'repeated' on the outward channel. It is a simple matter for the recipient to mark a message as read before resending it. This means that when the message arrives back at the sender, this mark can serve as an acknowledgement that the message was correctly received.

Ring networks consist of an unbroken circle of point-to-point connections of adjacent workstations. Messages travel from workstation to workstation in a round robin fashion. Workstations are connected to the cable through an access unit which is connected to a repeater which, in turn, retransmits messages addressed to other workstations.

In order to receive messages, each workstation must be capable of recognising its own address. However, no routing capability is required as messages automatically travel to the next workstation on the network. Originally, information flow on the ring was strictly in one direction. Now, two channel rings transmit information in different directions on each of the two channels.

When a ring topology is used to distribute control in local networks, the protocol used with it must avoid conflicting demands for shared channel.

A loop (see Figure 3.5) is a ring network using centralised control. One workstation will be designated as server, responsible for access to and control over the channel.

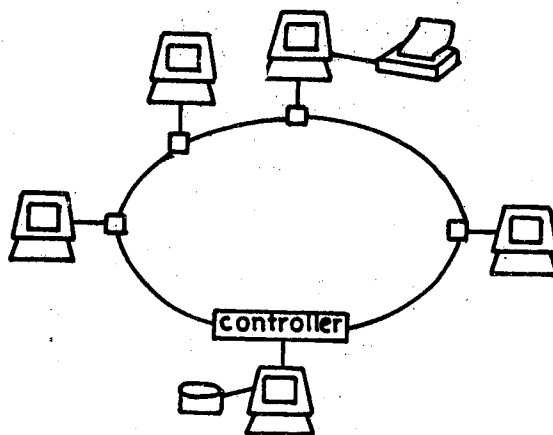


Fig. 3.5 : Loop

In practice, ring networks have been designed as single loops. Theoretically, a ring network could consist of several interconnected rings and form two or more hierarchical levels.

Advantages of the Ring

1. **Short cable length:** The amount of cabling involved in a ring topology is comparable to that of a bus and is small relative to that of a star. This means

that less connections will be needed, which will in turn increase network reliability.

2. **No wiring closet space required:** Since there is only one cable connecting each node to its immediate neighbours, it is not necessary to allocate space in the building for wiring closets.
3. **Suitable for optical fibres:** Optical fibres offer the possibility of very high speed transmission. Because traffic on a ring travels in one direction, it is easy to use optical fibres as a medium of transmission. Also, since a ring is made up of nodes connected by short segments of transmission medium, there is a possibility of mixing the types used for different parts of the network. Thus, a manufacturing company's network could use copper cables in the office area and optical fibres in the factory areas, where electrical interference may be a problem.

Disadvantages of the Ring

1. **Node failure causes network failure:** The transmission of data on a ring goes through every connected node on the ring before returning to the sender. If one node fails to pass data through itself, the entire network has failed and no traffic can flow until the defective node has been removed from the ring.
2. **Difficult to diagnose faults:** The fact that failure of one node will affect all others has serious implications for fault diagnosis. It may be necessary to examine a series of adjacent nodes to determine the faulty one. This operation may also require diagnostic facilities to be built into each node.
3. **Network reconfiguration is difficult:** The all or nothing nature of the ring topology can cause problems when one decides to extend or modify the geographical scope of the network. It is not possible to shut down a small section of the ring while keeping the majority of it working normally.
4. **Topology affects the access protocol:** Each node on a ring has a responsibility to pass on data that it receives. This means that the access protocol must take this into account. Before a node can transmit its own data, it must ensure that the medium is available for use.

Ring Evaluation Factors

- **Application:** A ring is good in situations where capacity must be allocated equally or where a small number of workstations operating at high speeds over short distances are to be connected.
- **Complexity:** A ring requires relatively complex hardware to implement. Message routing, on the other hand is simple: since only one message path is possible, the sending workstation need only know an address for the destination workstation. Routing information is not necessary.
- **Performance:** Performance under heavy traffic remains stable with less delay and degradation of service than other networks. Average transmission delays are

long, however, even under light traffic. Actual performance is dependent on the control protocols implemented.

- **System overhead:** Duplication of resources or a method of bypassing failure points is needed if the ring is to keep functioning when equipment fails.
- **Vulnerability:** Failure in a single workstation or in the channel can cause system failure because of the interdependence of workstations. Locating a failed repeater is particularly difficult; in a system with wide geographical distribution it may not be possible to immediately repair or circumvent the problem.
- **Expandability:** It is moderately easy to add or delete workstations on a ring network without making numerous connections for each change. Therefore, system modification costs are relatively low. Expansion does disrupt the whole system, even though it may be only briefly.

HYBRID TOPOLOGIES

By modifying or combining some of the characteristics of the 'pure' network topologies, a more useful result may be obtained. These combinations are called hybrid topologies.

TREE TOPOLOGY

The tree topology is a variant of the bus. The shape of the network is that of an inverted tree with the central root branching and sub branching to the extremities of the network (see Figure 3.6). It is normally implemented using coaxial cable as the transmission medium and broadband transmission techniques. One of the best known example is IBM's Personal Computer Network.

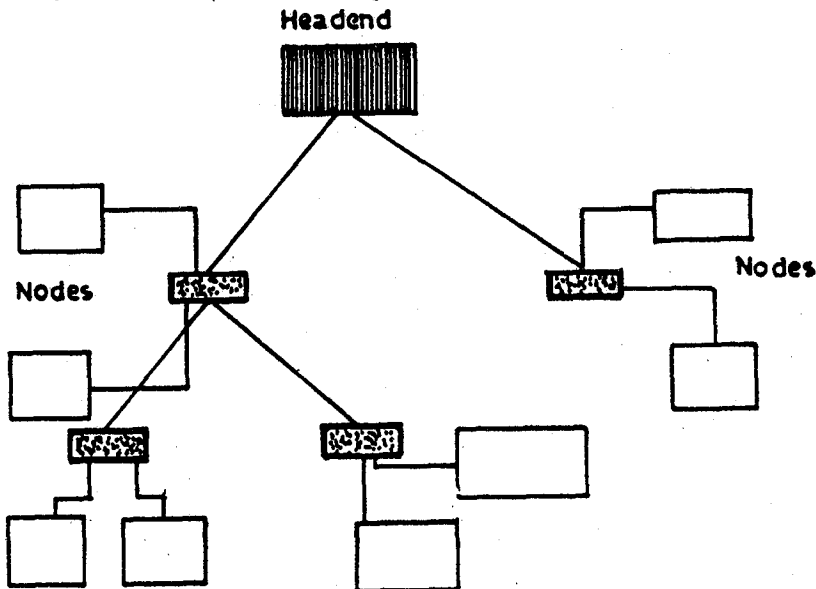


Fig. 3.6 a : The tree topology

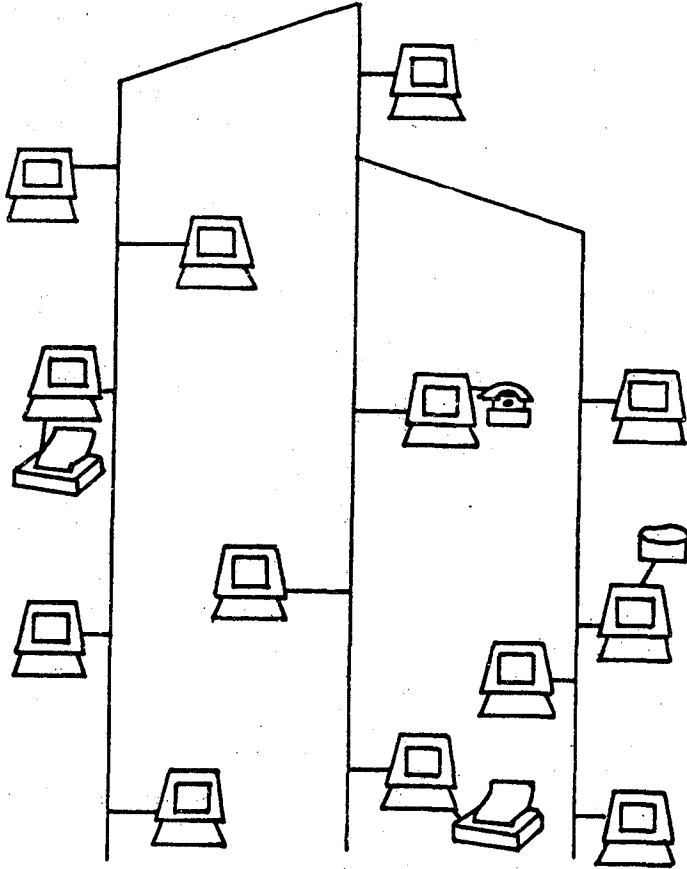


Fig. 3.6 b : Tree

Technically, a tree is a bus network comprised of a main cable which connects floors in a building (or several buildings), and branches which connect individual workstations in a more limited area. In effect, the network is divided into different segments. This topology is sometimes called a rooted tree and is used to refer to a network employing broadband coaxial cable. An unrooted tree is a baseband network and corresponds to the general definition of bus. Popularly, the terms tree and bus are used interchangeably.

The main difference between this type of network and one made of several bus segments is the presence of a 'root' to the tree. When a node transmits, the root (or 'headend' as it is sometimes called) receives the signal and rebroadcasts it through the entire network. In this way, repeaters are no longer necessary.

The pros and cons of the tree are very much the same as those of the bus, but there are some extra advantages and disadvantages.

Advantages of the Tree

1. **Easy to extend:** Because the tree is, of its very nature, divided into subunits, it is easier to add new nodes or branches to it.
2. **Fault isolation:** It is possible to disconnect whole branches of the network from the main structure. This makes it easier to isolate a defective node.

Disadvantages of the Tree

1. **Dependent on the root:** If the 'headend' device fails to operate, the entire network is rendered inoperable. In this respect, the tree suffers from the same reliability problems as the star.

STAR-RING TOPOLOGY

It has been seen that all of the 'pure' network topologies have associated advantages and disadvantages. In the star-ring, two topologies have been combined with the aim of achieving the best of both.

The configuration consists of a number of concentration points connected together in a ring. These concentration points would, in practice, consist of wiring closets located on each floor of a building. From each closet, nodes are connected in a star configuration, using some or all of the connection points.

Electrically, the star-ring operates exactly in the same way as a normal ring. The difference is that the physical wiring is arranged as a series of interconnected stars. Because of this, this topology is sometimes more descriptively called the star-shaped ring.

Star-shaped rings (see Figure 3.7), in which the cable between workstations passes through a central wire centre, have been gaining favour because of the need to keep the ring operating when a device or the cable fails. Automatic bypass relays which can be used to reconfigure network operations are located at the wire centre. If a failure occurs, the "dead" section of the ring may be effectively eliminated. Remaining workstations can keep operating. The star-shaped ring also facilitates maintenance by providing a centralised monitoring and reconfiguration point.

Advantages of the Star-ring

1. **Fault diagnosis and isolation:** The presence of concentration points in the network greatly eases fault diagnosis. If a fault is detected on the network, the initial problem is to find out which concentration point in the ring is to blame. The fact that this ring is quite small in relation to the total size of the network makes this problem more manageable. The offending concentration point can be isolated easily, leaving the network in a fully functional state while further fault diagnosis is carried out.
2. **Ease of expansion:** The modular construction of a star-ring network means that new sections may be easily added. When designing the network originally, each

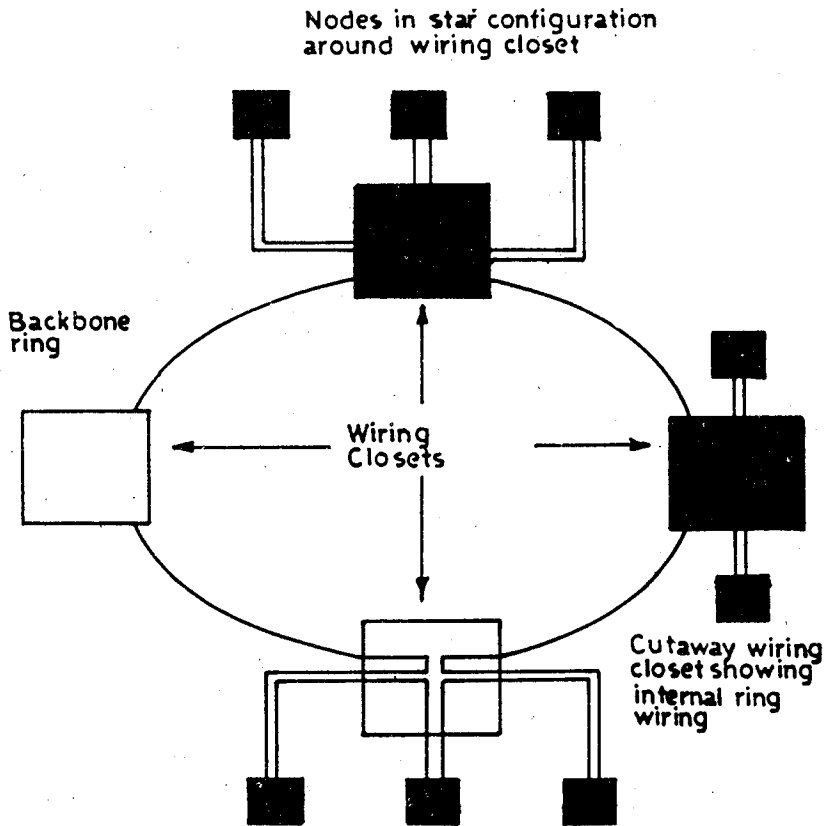


Fig. 3.7 a : The star-ring or star-shaped ring topology

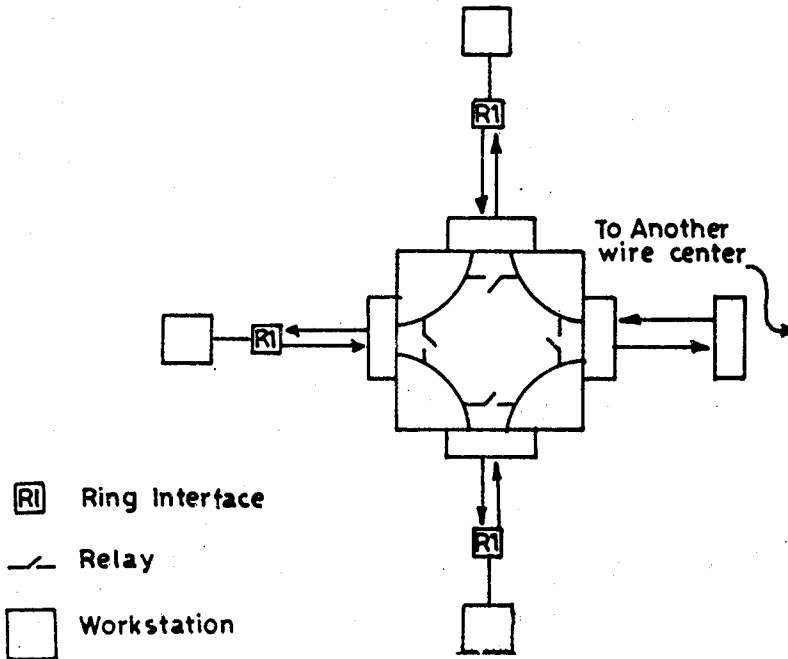


Fig. 3.7 b : Star-shaped Ring

concentration can have extra, unused lobes which can be called upon later, if needed. The next growth step involves adding a new concentration point and wiring it into the ring.

3. **Cabling:** The concentration points in a star-ring are connected via a single cable. This simplifies wiring between areas in an installation and cuts down on the congestion of cable ducts. Also, the wiring practices involved are very similar to that of telephone system installation. These techniques are well understood by building engineers and lend themselves well to the prewiring of buildings.

Disadvantages of the Star-ring

1. **Intelligent concentration points required:** Depending on the implementation used, the concentration points may need to have built-in intelligence/processing ability. This will be necessary if it is to assist in network fault diagnosis, node isolation or conversion from one form of transmission medium to another.
2. **Cabling:** The intercloset cabling in a star-ring is critical to its operation. This may mean that redundant cabling in the form of one or more back up rings may be necessary to meet reliability requirements. The largest section of the network (i.e., between the concentration points and the nodes) is laid out in a star. This means that a considerable amount of cable may be required.

CHOOSING A TOPOLOGY

In choosing a topology for a local area network, many factors must be considered. It must be easy to install both in existing buildings and those that are being prewired. Once installed, it must be able to cope with growth requirements. These may be sporadic and not well distributed geographically. It should be possible to carry out extensive changes to the network without completely depriving current users of service.

As with any other equipment, breakdowns in a LAN are to be expected. It is desirable to have a system where faults can be detected quickly and subsequently isolated, leaving the main section of the network operating normally.

The choice of topology can affect the range of possible media and the access method used to share it. Both of these can in turn affect the complexity and speed of operation of the individual nodes.

The star topology is of most interest from a historical point of view and also because it is the topology against which the others are measured. It is more appropriate for terminal-host configurations than for LANs. The remaining two 'pure' topologies both have good and bad points, some of which can be improved by combining them with other topologies.

TRANSMISSION MEDIA

Transmission lines, the backbone of the network, come in two basic varieties: baseband and broadband. Baseband communication links are twisted pair wire and

baseband coaxial cable. Broadband media are broadband coaxial and fibre optic cable. Description of the cables, along with the additional devices required to turn a piece of cable into a network, will occupy the rest of this section.

MEDIA EVALUATION FACTORS

Each media is better suited to certain types of installation than to others. Factors influencing media choice follow the descriptions of the media and network components. Topics covered include the following:

- **Application:** In what size installation is the media most appropriate? How great a distance can it cover easily?
- **Application restrictions:** Under what conditions should the media be avoided?
- **Topology:** Which topologies use the cable?
- **Attraction:** In what situation is the cable to be preferred?
- **Network Reliability:** How dependable is the necessary equipment (other than the microcomputer workstations and the network interface cards)?
- **Vulnerability:** What are the major causes of equipment failure?
- **Susceptibility to noise:** How prone to interference is the network?
- **Implementation costs:** Installation of cabling and associated equipment is the great hidden cost of networking.

For all media, the cost of installation easily exceeds that of the cost of the wire itself.

- **Security:** How open to tapping is the media?

Tables 3.3 and 3.4 gives various factors or attributes for comparing the major media.

TABLE 3.3 : Comparing the Major Media

	Twisted pair wire	Baseband coaxial cable	Broad band coaxial cable	Fiber optic cable
Topologies supported	Ring, star, bus, tree	Bus, tree, ring	Bus, tree	Ring star, tree
Maximum number of nodes per network	Generally, up to 1024	Generally, up to 1024	Generally, up to 1024	Generally, up to 1024
Maximum geographical	3 kilometers	10 kilometers	50 kilometers	10 kilometers and up
Type of signal	Single-channel, unidirectional, analog or digital, depending on type of modulation used, half- or full-duplex	Single channel, bidirectional, digital, half-duplex	Multi-channel unidirectional RF analog, half-duplex (full-duplex can be achieved by using	One single-channel, unidirectional, half-duplex, signal-encoded lightbeam per fiber; multiple fibers per cable; full-

			two channels or two cables	duplex can be achieved by using two fibers
Maximum bandwidth	Generally, up to 4 Mbps	Generally, up to 10 Mbps	Up to 499 MHz (aggregate total)	Up to 50 Mbps in 10 kilometer range, up to 1 Gbps in experimental tests
Major advantages	Low cost May be existing plant; no rewiring needed; very easy to install	Low maintenance cost Simple to install and tap	Supports voice, data, and video applications simultaneously Better immunity to noise and interference than baseband More flexible topology (branching tree) Rugged, durable equipment, needs no conduit Tolerates 100% bandwidth loading Uses off-the-shelf industry-standard CATV components	Supports voice, data, and video applications simultaneously Immunity to noise, crosstalk, and electrical interference Very high bandwidth Highly secure Low signal loss Low weight diameter; can be installed in small spaces Durable under adverse temperature, chemical, and radiation conditions
Major disadvantages	High error rates at higher speeds Limited bandwidth Low immunity to noise and crosstalk Difficult to maintain, troubleshoot Lacks physical ruggedness, requires conduits, trenches, or ducts	Lower noise immunity than broadband (can be improved by the use of filters, special cable and other means) Bandwidth can carry only about 40% load to remain stable Limited distance and topology Conduit required for hostile environments	High maintenance costs More difficult to install and tap than baseband RF modems required at each user station; modems are expensive and limit the user device's transmission rate; complex initial engineering	Very high cost, but delining Require skilled installation and maintenance personnel Experimental technology; limited commercial availability Currently limited to point-to-point connections
Bandwidth (partial)	Low	Moderate	High	Very High
Data Transfer Reliability	Low	High	High	Very High
Noise Susceptibility	High	Moderate	Low	None
Transmission Security	Low	Low	Low	High
Length	Low	Moderate	High	Very High
Installation	Easiest	Hard	Hardest	Moderate

TABLE 3.4 : Transmission Media Alternatives

	Twisted Pair	Coax	Optical Fiber
Proven technology	Yes	Yes	Yes
Two-way	Yes	Yes	Yes
Availability	Yes	Yes	Limited
Maintainability	Yes	Yes	Limited
Reliability	High	High	High
Expandability	Limited	High	Very high
Immunity to :			
radio frequency			
interference	No	No	Yes
power line			
interference	No	No	Yes
electromagnetic statis	No	No	Yes
cross-talk	No	No	Yes
Bit error rate (BER)	High	Medium	Very low
Bandwidth			
Up to 24 64 Kbps			
channels	Yes	Yes	Yes
Up to 50 video			
channels	No	Yes	Yes
Beyond 150 video			
channels	No	No	Yes
Ability to use system for power	Limited	Yes	No
Technical support required	Low	Medium	High
Electronics costs	Low	Medium	High
Overall system price	Low	Medium	High
Estimated construction costs per mile:			
Aerial	\$13,000	\$15,000	\$20,000
Underground	\$23,000	\$25,000	\$40,000
Installation cycle in days	90	120	120
Third-party disruption	Yes	Yes	No
Workman safety	Low	Low	Very high
Impact by weather	Medium	Medium	Low
Geographic penetration	High	Medium	Limited

TWISTED PAIR WIRE

Twisted pair wire (see Figure 3.8) is familiar as the cable used for telephone systems. Since the start of the computer age, it has been used to connect terminals and other low-speed data equipment to the mainframe. Use of twisted pair wire is so widespread that it is frequently pre-installed in buildings.

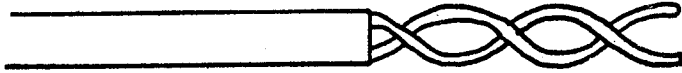


Fig. 3.8 : Twisted Pair Wire

As the name implies, pairs of wires are spiralled about each other. Gauge (size) of the base wire varies, as does the number of twists per foot. The twisting standardises the electrical properties throughout the length of the cable and minimises the interference created by adjacent wires in multipair cable. Normally, copper is used for the wire. Twisted pair tends to be unshielded or only minimally shielded. As a result, the cable is light and relatively easy to install.

Components of a Twisted Pair Network

A twisted pair wire network (see Figure 3.9) consists of the main cable, plus the following:

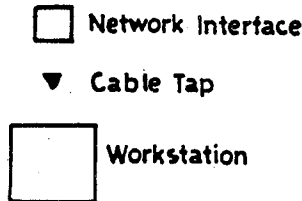
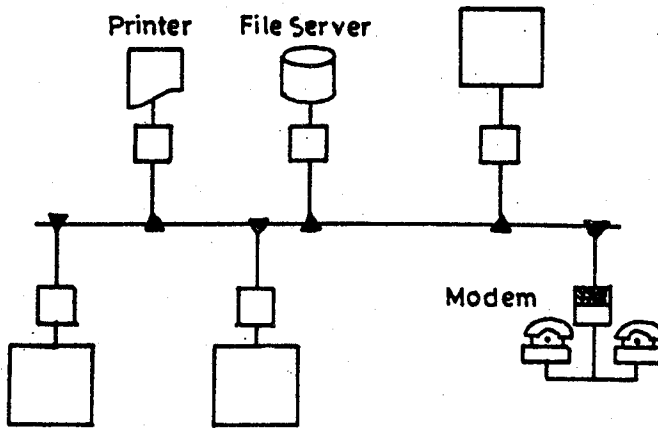


Fig. 3.9 : Twisted Pair Network

- **Transceivers:** Network interface units which provide the intelligence for reading message addresses and for other network-oriented communication functions.
- **Cable taps:** Connect the transceiver to the main cable.
- **Repeaters:** Boost the strength of the signal as the messages pass from one cable section to another. The distance unamplified digital signals can travel on twisted pair is limited — approximately 8,000 feet under favourable conditions, without a repeater. The higher the speed of the signal, the shorter the distance it can travel.

Twisted Pair Evaluation Factors

- **Application:** Twisted pair cable is most suitable for point- to-point applications where low speed, low demand devices are interconnected. Average data rates are severely restricted, dropping rapidly as the distance between devices increases.
- **Application restrictions:** Most implementations restrict the number of workstations on the lines and limit distances to the area within a single building.
- **Topology:** Twisted pair is used in star, bus and ring topologies.
- **Attraction:** One major attraction of twisted pair is its wide use for other communication purposes, particularly telephone networks. A second attraction is cost: wiring and installation are relatively inexpensive. To date, it has been the main transmission medium for local network.
- **Network Reliability:** Reliability is excellent. How often does your in-house telephone system fail because of cabling problems?
- **Vulnerability:** Although the medium is extremely flexible, physical ruggedness is low. Twisted pair is susceptible to damage from improper installation, sharp bends and contact with rough surfaces.
- **Susceptibility to noise:** Lack of shielding leaves the medium vulnerable to interference from electrical noise, resulting in high error rates. Twisted pair wire should not be routed near any device that has a strong electromagnetic field, such as a radio transmitter or power transformer. Electric motors, gasoline engines, industrial machinery also must be avoided.
- **Implementation costs:** Cable cost depends on the number of twists per foot; the type of insulation and shielding; and the guage of the wire. Based on cable costs alone, twisted pair is the least expensive medium. Additionally, it already is installed in many buildings. If not, or in cases where existing wiring cannot be used, installation costs are moderate, slightly less than that of coaxial cable.
- **Security:** Twisted pair networks are severely deficient in security due to lack of shielding. Electrical signals on the network are broadcast and may be intercepted by stations not actually connected to the network.

BASEBAND COAXIAL CABLE

Coaxial cable has been used for many years in the telephone network in applications with requirements similar to those of a LAN. It also is used for CATV (Community Antenna Television) systems. Both baseband and broadband coaxial cable are available. Although they are similar in construction, their installation and applications differ. Therefore, they will be discussed in separate sections.

In baseband coaxial cable (see Figure 3.10), a central carrier wire is surrounded by a fine woven mesh of copper which forms an outer shell. The space between the wire and the outer shell is insulated to separate the two conductors and to maintain the electrical properties. The entire cable is covered by protective insulation to minimise electrical emissions. The cable is usually approximately 3/8 inch diameter.



Fig. 3.10 : Baseband Coaxial Cable

The cable carries a single digital signal at a very high data rate — up to 10 to 12 megabits per second. Transmission frequency is relatively low. Bits are put directly on the cable without modulation.

Components of a Baseband Coaxial Network

In most respects, baseband coaxial is similar to twisted wire pairs. To transform a simple cable into a network (see Figure 3.11), the following parts are needed:

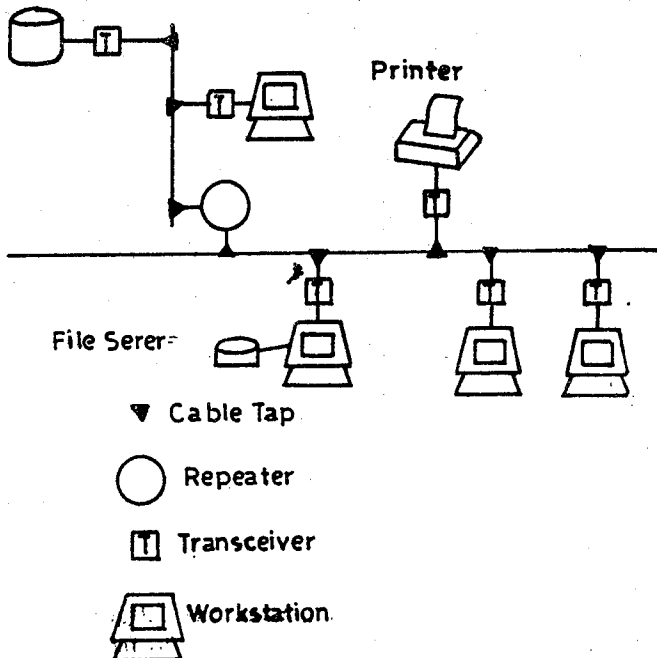


Fig. 3.11 : Baseband Coaxial Network

- **Transceivers:** Network interface units, which provide the intelligence for reading message addresses and for other network-oriented communication functions.
- **Cable taps:** Connect the transceiver cable to the main cable.
- **Repeaters:** Amplify the signal as the messages pass from one cable section to another.

The main network cable is installed in a wire trough, which may be located beneath a raised floor, inside walls or above a dropped ceiling. Local outlets may be provided in each office to facilitate connecting an individual workstation to the network.

Baseband Coaxial Evaluation Factors

- **Application:** Baseband coaxial cable may be interchanged with twisted pair for many, but not all, purposes.
- **Application restrictions:** Most baseband coaxial networks limit the distance covered and the number of workstations.
- **Topology:** Baseband coaxial cable is frequently used for bus networks.
- **Attraction:** Baseband coaxial offers greater resistance to noise and better performance than twisted pair for an only slightly higher cable cost.
- **Network Reliability:** Reliability is good to excellent.
- **Vulnerability:** The cable itself is physically rugged.
- **Susceptibility to noise:** Although less susceptible to electrical noise than twisted pair, it is still noise sensitive. Baseband coaxial cable is not recommended for installation in sites with high levels of electrical noise.
- **Installation costs:** Installation costs are comparable to twisted pair.
- **Security:** Security of baseband coaxial is a problem; the cable may act as an antenna, broadcasting the signal, inadvertently permitting unauthorised tapping. The broadcast signal may interfere with radio, television and other broadcast systems located nearby.

BROADBAND COAXIAL CABLE

Broadband coaxial cable (see Figure 3.12) comes in several different diameters with varying amounts of insulation. The cable may have the same construction as baseband coaxial, or the central carrier may be surrounded by an aluminium sleeve.



Fig. 3.12 : Broadband Coaxial Cable

The space between the core and the shell is filled with insulation, and the whole is enclosed in a protective coat of insulation. Broadband coaxial cable can carry 50 to 100 television channels or thousands of voice and low speed data channels at rates of 9.2 to 50 kilobits per second.

Components of a Broadband Coaxial Network

Broadband coaxial networks (see Figure 3.13) usually are implemented with off-the-shelf CATV hardware. The radio frequency signal carrier propagates in one direction only. Table 3.5 gives a comparative analysis of baseband versus broadband.

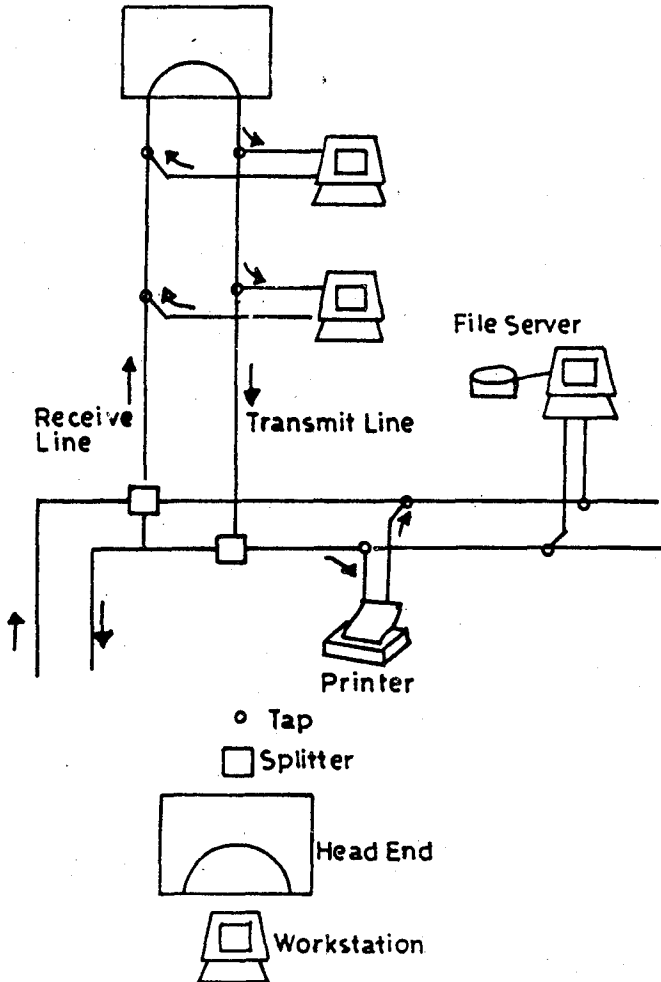


Fig. 3.13 : Broadband Coaxial Network

TABLE 3.5 : Baseband versus Broadband

Advantages	Disadvantages
<i>Baseband</i>	
Cheaper-no modem Simpler technology Easy to install	Single channel Limited capacity Limited distance Grounding concerns
<i>Broadband</i>	
High capacity Multiple traffic types More flexible configurations Large area coverage Mature CATV technology	Modem cost Installation and maintenance complexity Doubled propagation delay

If the system uses a single cable, the signal is divided into inbound (transmit) and outbound (receive) frequency ranges. Workstations receive messages within the outbound frequency range and transmit within the inbound frequency range. A translator at the head end converts inbound frequencies to outbound frequencies. On a 300 MHz or 400 MHz line, 40 to 50 channels of 6 MHz can be provided.

For local area networks, approximately one-half of the available channels are used for each direction, a scheme called Mid-split. The "split" in the name refers to the placement of unassigned frequencies, required as guardband to minimise interference.

The head end, located at the midpoint of the single cable, serves as the point of origin of all radio frequency signals and the collection point for all signals being generated on the network. It acts as the inbound-outbound cross-over point which divides the network into a transmit half and a receive half. Shared devices frequently are located at the cable head end. As noise also returns to the head end, the return signals may be subject to noise degradation.

In a dual cable system, one cable carries inbound transmissions, the other outbound transmissions. The head end passes signals from the inbound line to the outbound line across all frequencies. Workstations send and receive on the same frequency, but on different cables.

In both systems, when the network cable is installed, the two halves are positioned parallel and physically adjacent to each other. Operational differences between LANs using mid-split single cable and dual cable systems are minor.

The coaxial network contains three levels of line:

Trunk: The main network cable, which transports radio-frequency signals between amplifiers. Each floor in a multi-floor installation will have a trunk cable. It also is used for long runs between buildings. Trunk cable is normally thicker and more rigid than other cables in the network.

- **Branch:** Carries the network to the general area of the user. Branch distribution cables may extend from other branches, subject only to signal quality considerations.
- **Drop:** Connects the user outlet to the branch. The cable used is thin and more flexible than other broadband coaxial cables. Several drop cables may be attached to each connector.

The cable is installed above a dropped ceiling or below a false floor where it can be "pulled" into position. Risers bring the main cable from one floor to another. Usually a building will have only two riser cables. Each floor will have a pair of trunk cables split at various points into branches. The cable may be buried for runs between buildings or hung on poles (as is done for CATV).

To the lines are connected:

- **Radio-Frequency Modems:** Used as network interface. Broadband systems require modems to translate the data onto and off the carrier signal. The modem must be able to transmit and/or receive on a variety of frequencies and is therefore sometimes called frequency-agile.
- **Amplifiers:** Used to "boost" the signal. Amplifiers (also called Repeaters) are necessary over long distances, such as an installation encompassing multiple floors of a building or multiple buildings.
- **Power supply:** The system as a whole runs on electrical power. Distributing power over the coaxial cable eliminates the need for a separate power supply at each amplifier location, resulting in greater flexibility in the placement of amplifiers. For reliability, electrical grounding is necessary.
- **Directional couplers:** Insure that signals transmitted by any network device will be transmitted only toward the head end.
- **Splitters and combiners:** Permit branching of cable.
- **Terminators:** End a line. Terminators limit noise reflection in the system and minimise undesirable signals.

To run the system, a power supply is necessary. Power may be provided at the head end or with a power outlet at each amplifier.

In installations where user outlets have been liberally supplied, adding workstations or moving existing workstations from one location to any other location served by the network is achieved easily. In many cases, connection and/or disconnection of a workstation will not affect the operation of the network as a whole. Reconfiguration of the network into a hierarchy with subnetworks is possible.

Broadband Coaxial Evaluation Factors

- **Application:** Coaxial cable is preferred for high-frequency, wide bandwidth, high-speed applications. It is currently the most practical choice for networks covering moderate distances; requiring digital, voice and video transmission; and/or having a large number of workstations.

- **Application restrictions:** The cost of the system makes broadband coaxial impractical for small networks.
- **Topology:** Basic broadband coaxial topology is extremely flexible. Star or tree are suggested by the transmission technology.
- **Attraction:** All transmission devices are readily available

CATV components with proven high reliability.

- **Network Reliability:** The basic technology is highly dependable. Network reliability depends on the reliability of individual parts. Cable amplifiers tend to be the major point of failure, particularly when new. If amplifiers survive the first several months, they usually do not fail until near end of guaranteed life.
- **Vulnerability:** The cable is susceptible to damage from careless installation, improperly installed devices and failure in cable components. It cannot make sharp bends around corners. In addition, the cable is sensitive to temperature changes.
- **Susceptibility to noise:** Transmission is susceptible to interference from low-frequency electromagnetic noise. The actual noise immunity is dependent on the physical location and method of implementation. Coaxial cable can be used in many environments where twisted pair wire or other unshield-ed cable could not be used.
- **Implementation costs:** While the cable itself is not expensive, system costs are high because of initial equipment and upkeep costs. Installation and maintenance of CATV equipment is routine.
- **Security:** Unlike baseband coaxial, broadband coaxial cable does not broadcast the electrical signals that it carries. Security, however, still may be a problem: coaxial cable can be easily tapped by anyone who can gain physical access to the cable.

FIBRE OPTIC CABLE

Fibre optic cable (see Figure 3.14) is a relatively new medium for local area networks. Light signals are transmitted through a cable/waveguide composed of a bundle glass or plastic fibres. Each individual strand has a centre core of plastic or glass with a high refractive index, surrounded by a cladding layer (overcoat) with a slightly lower index. The cladding layer isolates the fibres and prevents interference

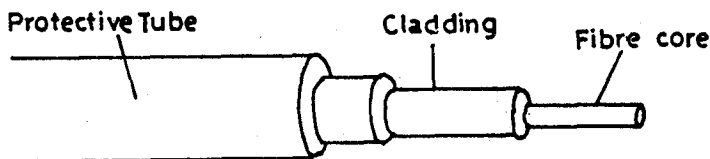


Fig. 3.14 : Fibre Optic Cable

between adjacent strands, as well as providing some physical protection for the core. The whole usually is enclosed by additional protective outer layers which play no role in the actual transmission.

Three basic types of cable are available:

- Single mode fibres have an extremely thin core diameter. While the thinness provides high performance, it makes connection to light transmitters and other cable segments extremely difficult.
- Stepped index fibres contain a core of high resolution within a shell of lower resolution. The boundary between core and cladding is abrupt. Connections are easier than with other types of fibre.
- Graded index fibres vary in density from the core outward. The gradation moderates the dispersion of signals. Graded index fibre is currently the most commonly available, because it is preferred for telecommunications. It has the highest transmission rate of the three types of cable.

Table 3.6 gives a comparative analysis of three types of optical fibres. Figure 3.15 depicts the three optical fibre transmission modes.

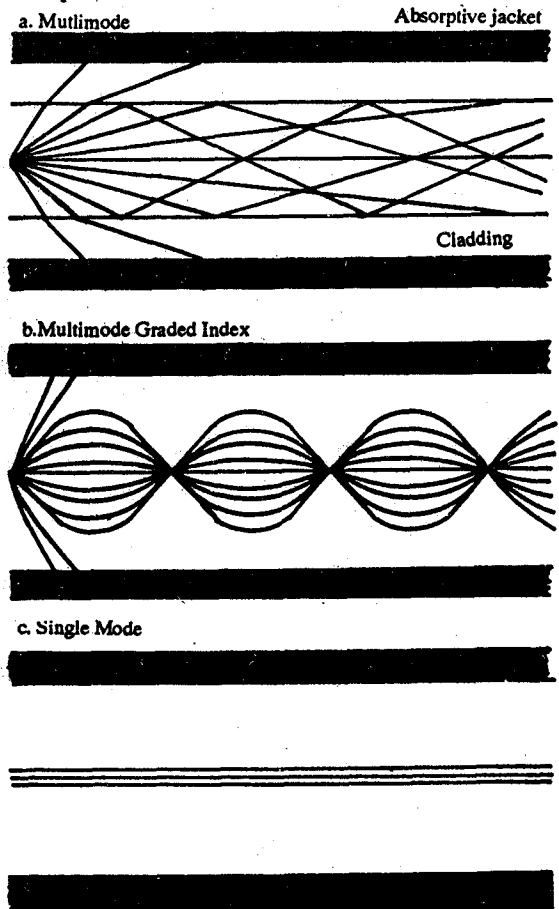


Fig. 3.15 : Optical Fiber Transmission Modes

TABLE 3.6 : Comparison of Three Types of Optical Fibers

	Step-index Multimode	Graded-Index Multimode	Single-mode
Light Source	Led or laser	Led or laser	laser
Bandwidth	wide (up to 200 MHz/km)	very wide (200 Mhz to 3 GHz/km)	extremely wide (3 GHz to 50 GHz/km)
Splicing	difficult	difficult	difficult
Typical Application	computer data links	moderate-length telephone lines	telecommunication long line
Cost	least expensive	more expensive	most expensive
Core Diamter (μm)	50 to 125	50 to 125'	2 to 8
Cladding Diameter (μm)	125 to 440	125 to 440	15 to 60

Cable segments must be aligned precisely for the signal to continue from one segment to the next, because light tends to travel in a wave-like motion rather than a straight line. The greater the fluctuations in the light wave, the more rapidly the performance degrades and the greater the dispersion of the signal. The thinner the optic and the narrower the light source, the straighter the wave is forced to travel and, therefore, the more efficient the network as a whole.

Components of a Fibre Optic Network

In addition to the cable, the fibre optic network (see Figure 3.16) requires the following:

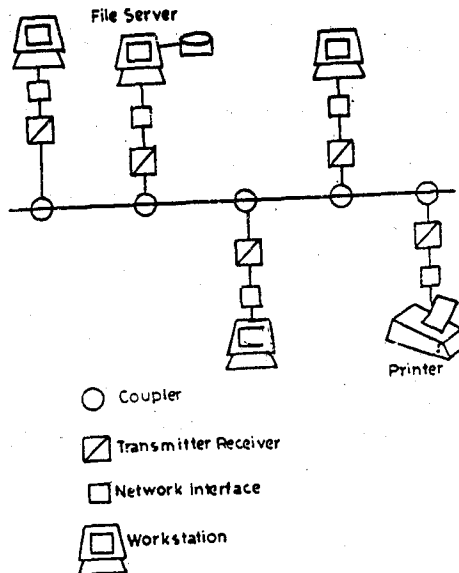


Fig. 3.16 : Fiber Optic Network

- **A Transmitter:** Consisting of a light source and a power supply. Light is supplied by either a LED (Light Emitting Diode) or a laser diode.
- **Receivers:** Also called detectors, which sense the light signals and convert them back to electrical signals.
- **Repeaters:** Necessary for very long networks. Fibre optic systems use far fewer repeaters than any other media.
- **Couplers and connectors:** Used to join two lengths of cable.

Any mating of fibre optic cable requires a great deal of care, because minor mismatches can cause a large loss of efficiency.

In operation, a workstation sends data in standard electrical form to a transmitter, where it is converted into light pulses. The light signals are collected by the waveguide and carried to a receiver. At the receiver, the light pulses are retranslated to electrical pulses and delivered to the destination workstation.

Unlike coaxial cable, fiber optic systems generally do not require repeaters over the distances typically found in LANs. Repeaterless runs of up to 4 kilometers or more can be accommodated, as compared to only 1 1/2 kilometers for coaxial cable.

The light signals may be digital or analog. Digital light signals are created by on/off pulses; analog signals use varying light intensity. Each cable can transmit in one direction only. Two-way communications require two optic cables.

Performance of the system is a function of transmission speed, bandwidth and the amount of signal dispersion or degradation, over the length of the cable. The wider the range of light wavelengths at the source, the sooner the signal disperses.

Fibre Optic Evaluation Factors

- **Application:** Fibre optic is particularly suited to systems with very-high speed data and video transmission requirements; for transmission over distances greater than other media can support; for installations which anticipate rapidly increasing demand for communication capabilities; and where space and signal interference cause problems.
- **Application restrictions:** Fibre optic is not suitable for small installations or where cost is a major factor.
- **Topology:** Currently, fibre optic systems are most suitable for point-to-point transmission, suggesting star or ring topologies. Bus topology is possible, but currently is infrequently implemented.
- **Attraction:** Fibre optic networks support an extremely high data rate — over 1 gigabit per second (10 to the 9th power bits per second) — on a potentially unlimited bandwidth, with extremely high reliability and high quality output. Fibre optic cable is thin, light weight, very flexible and extremely resistant to ordinary transmission hazards.

- **Network Reliability:** Fibre optic cable is rugged, has a long life and has displayed high reliability under adverse physical conditions.
- **Vulnerability:** Fibre optic networks are susceptible to signal loss from improper splicing or interfacing, bending and pressure. The light source may be heat sensitive.
- **Susceptibility to noise:** Due to its resistance to electrical, electromagnetic and radio frequency noise, fibre optic may be the only functional choice for a heavily industrial installation. The fibre optic cable is electrically isolated and therefore cannot broadcast its signal outside the network. It has the added advantage of not emitting sparks and thus does not present a potential fire hazard.
- **Implementation costs:** Currently fibre optic networks are very expensive. Installation and equipment costs, particularly of coupling and interfacing devices, are high. The installation is complex, especially as connections must be precise. However, costs of all parts of the network are dropping rapidly and will continue to do so.
- **Security:** Fibre optic is the best choice where light security is mandatory. It is virtually invulnerable to tapping.

RELATIONSHIP BETWEEN MEDIUM AND TOPOLOGY

The choice of transmission medium and topology are not independent. Table 3.7 shows the preferred combinations. The ring topology requires point-to-point links between repeaters. Twisted-pair wire, baseband coaxial cable and optical fibre can all be used to provide the links. However, broadband coaxial cable would not work well in this topology. Each repeater would have to be capable of receiving and transmitting data simultaneously on multiple channels. It is doubtful that the expense of such devices could be justified. Table 3.8 summarises representative parameters of transmission media for commercially available ring LANs.

TABLE 3.7 : Relationship Between Medium and Topology

Medium	Topology			
	Bus	Tree	Ring	Star
Twisted par	x		x	x
Baseband coaxial cable	x		x	
Broadband coaxial cable	x	x		
Optical fiber			x	

TABLE 3.8 : Characteristic for Transmission Media for Local Networks : Ring

Transmission Medium	Data Rate (Mbps)	Spacing	Number of Repeaters
Unshielded Twisted Pair	4	0.1	72
Shielded Twisted Pair	16	0.3	250
Baseband Coaxial Cable	16	1.0	250
Optical Fiber	100	2.0	240

For the bus topology, twisted pair and both baseband and broadband coaxial cable are appropriate. At the present time, optical fibre cable is not feasible, as the multipoint configuration is not cost-effective, due to the difficulty in constructing low-loss optical taps. The tree topology can be employed with broadband coaxial cable. The unidirectional nature of broadband signalling allows the construction of a tree architecture. On the other hand, the bidirectional nature of baseband signalling, on either twisted pair or coaxial cable, is not suited to the tree topology. Again optical fibre is not now cost effective for the multipoint nature of the tree topology. Table 3.9 summarises representative parameters for transmission media for commercially available bus and tree LANs.

TABLE 3.9 : Characteristic for Transmission Media for Local Networks : Bus

Transmission Medium	Data Rate (Mbps)	Range (km)	Number of Taps
Unshielded Twisted Pair	1-2	<2	10's
Baseband Coaxial Cable	10/70	<3/<1	100's/10's
Broadband Coaxial Cable	20 per channel	<30	100's-1,000's

The reader will note that the performance for a given medium is considerably better for the ring topology compared with the bus/tree topology. In the bus/tree topology, each station is attached to the medium by a tap, and each tap introduces some attenuation and distortion to the signal as it passes by. In the ring, each station is attached to the medium by a repeater, and each repeater generates a new signal to compensate for effects of attenuation and distortion.

The star topology requires a single point-to-point link between each device and the central switch. Twisted pair is admirably suited to the task. The higher data rates of coaxial cable or fibre would overwhelm the switches of today's technology.

COMMUNICATION SWITCHING TECHNIQUES

So far we have discussed how data can be encoded and transmitted over a communication link. In its simplest form, data communication takes place between two devices that are directly connected by some form of transmission medium. Often, however, it is impractical for two devices to be directly connected. This is so for one (or both) of the following contingencies:

- The devices are very far apart. It would be inordinately expensive, for example, to string a dedicated link between two devices, thousands of miles apart.
- There is a set of devices, each of which may require a link to many of the others at various times. Examples are of all the telephones in the world and all of the terminals and computers owned by a single organisation. Except for the case where very few devices are available, it is impractical to provide a dedicated wire between each pair of devices.

The solution to this problem is to attach each device to a communication network. Communication is achieved by transmitting data from source to destination through a network of intermediate nodes. These nodes are not concerned with the content of the data; rather their purpose is to provide a switching facility that will move the data from node to node until they reach their destination. Figure 3.17 illustrates the situation. We have a collection of devices that wish to communicate; we will refer to them generically as **stations**. The stations may be computers, terminals, telephones or other communicating devices. We also have a collection of devices whose purpose is to provide communication, which we will refer to as **nodes**. The nodes are connected to each other in some fashion by transmission links. Each station attaches to a node. The collection of nodes is referred to as a **communication network**. If the attached devices are computers and terminals, then the collection of nodes plus stations is referred to as a **computer network**.

Three switching techniques are in common use:

- Circuit switching
- Message switching
- Packet switching

CIRCUIT SWITCHING

Communication via circuit switching implies that there is a dedicated communication path between two stations. That path is a connected sequence of links between nodes. On each physical link, a channel is dedicated to the connection. The most common example of circuit switching is the telephone network. Figure 3.18a illustrates the concept of circuit switching.

Communication via circuit switching involves three phases, which can be explained with reference to Figure 3.17.

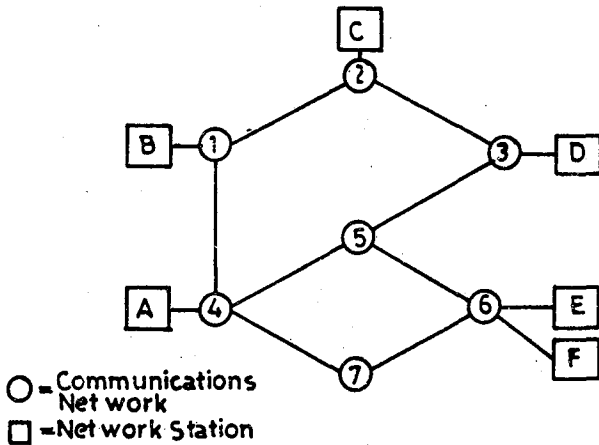


Fig. 3.17 : Generic Switching Network

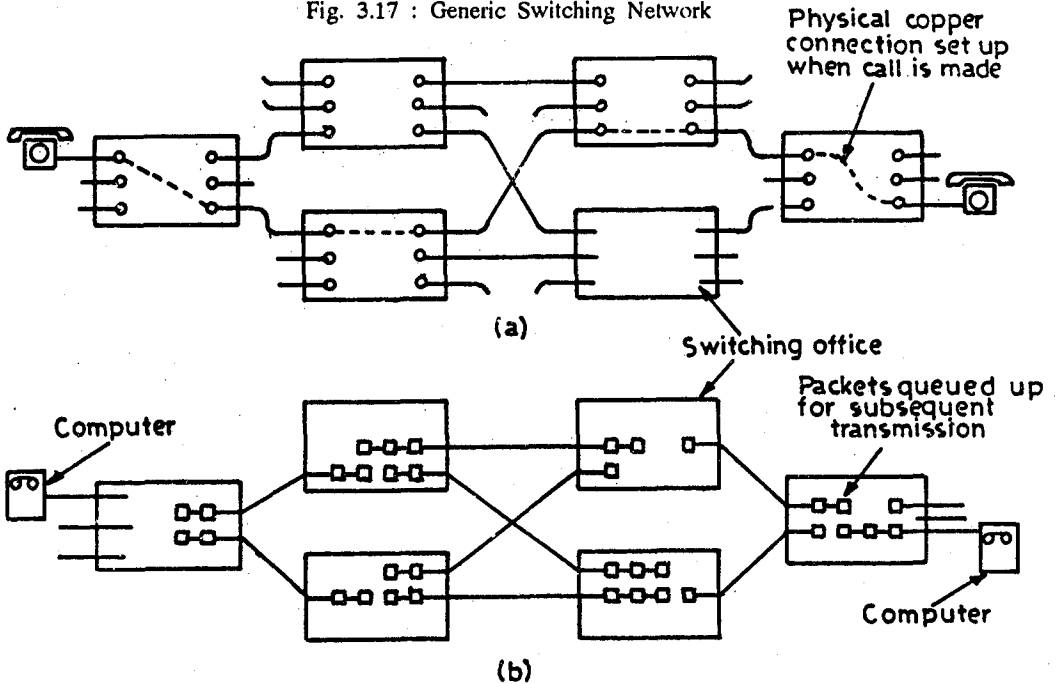


Fig. 3.18 (a) : Circuit switching. (b) : Packet switching

1. **Circuit establishment:** Before any data can be transmitted, an end-to-end (station-to-station) circuit must be established. For example, station A sends a request to node 4 requesting a connection to station E. Typically, the circuit from A to 4 is a dedicated line, so that part of the connection already exists. Node 4 must find the next leg in a route leading to node 6. Based on routing

information and measures of availability and perhaps cost, node 4 selects the circuit to node 5, allocates a free channel (using TDM or FDM) on that circuit and sends a message requesting connection to E. So far, a dedicated path has been established from A through 4 to 5. Since a number of stations may attach to 4, it must be able to establish internal paths from multiple stations to multiple nodes. The remainder of the process proceeds similarly. Node 5 dedicates a channel to node 6 and internally ties that channel to the channel from node 4. Node 6 completes the connection to E. In completing the connection, a test is made to determine if E is busy or is prepared to accept the connection.

2. **Data transfer:** Signals can now be transmitted from A through the network to E. The data may be digital (e.g.terminal to host) or analog (e.g.voice). The signalling and transmission may each be either digital or analog. In any case, the path is : A-4 circuit, internal switching through 4, 4-5 channel, internal switching through 5, 5-6 channel, internal switching through 6 and 6-E circuit. Generally, the connection is full duplex and data may be transmitted in both directions.
3. **Circuit disconnect:** After some period of data transfer, the connection is terminated, usually by the action of one of the two stations. Signals must be propagated to 4, 5 and 6 to deallocate the dedicated resources.

Note that the connection path is established before data transmission begins. Thus channel capacity must be available and reserved between each pair of nodes in the path and each node must have internal switching capacity to handle the connection. The switches must have the intelligence to make these allocations and to device a route through the network.

Circuit switching can be rather inefficient. Channel capacity is dedicated for the duration of a connection, even if no data are being transferred. For a voice connection, utilisation may be rather high, but it still does not approach 100%. For a terminal-to-computer connection, the capacity may be idle during most of the time of the connection. In terms of performance, there is a delay prior to data transfer for call establishment. However, once the circuit is established, the network is effectively transparent to the users. Data are transmitted at a fixed rate with no delay other than the propagation delay through the transmission links. The delay at each node is negligible.

Message Switching

Circuit switching is an appropriate and easily used technique in the case of data exchanges that involve a relatively continuous flow, such as voice (telephone) and some forms of sensor and telemetry input. However, circuit switching does have two drawbacks:

- Both stations must be available at the same time for the data exchange.
- Resources must be available and dedicated through the network between the two stations, when available.

An alternative approach, which is generally appropriate to digital data exchange, is to exchange logical units of data, called messages. Examples of messages are telegrams, electronic mail, computer files and transaction queries and responses. If one thinks of data exchange as a sequence of messages being transmitted in both directions between stations, then a very different approach, known as message switching, can be used.

With message switching, it is not necessary to establish a dedicated path between two stations. Rather, if a station wishes to send a message (a logical unit of information) it appends a destination address to the message. The message is then passed through the network from node to node. At each node, the entire message is received, stored briefly and then transmitted to the next node.

In a circuit-switching network, each node is an electronic or perhaps electro-mechanical switching device which transmits bits as fast as it receives them. A message-switching node is typically a general-purpose minicomputer, with sufficient storage to buffer messages as they come. A message is delayed at each node for the time required to receive all bits of the message plus a queuing delay waiting for an opportunity to retransmit to the next node.

Again using Figure 3.17, consider a message from A to E. A appends E's address to the message and sends it to node 4. Node 4 stores the message and determines the next leg of the route (say to 5). Then node 4 queues the message for transmission over the 4-5 link. When the link is available, the message is transmitted to node 5, which will forward the message to node 6 and finally to E. This system is also known as a **store-and-forward** message system. In some cases, the node to which the station attaches or some central node, also files the message, creating a permanent record.

The advantages of this approach over circuit switching are:

- Line efficiency is greater, since a single node-to-node channel can be shared by many messages over time. For the same traffic volume, less total transmission capacity is needed.
- Simultaneous availability of sender and receiver is not required. The network can store the message pending the availability of the receiver.
- When traffic becomes heavy on a circuit-switched network, some calls are blocked. On a message-switched network, messages are still accepted, but delivery delay increases.
- A message-switching system can send one message to many destinations. This facility is not easily provided by a circuit-switched network.
- Message priorities can be established.
- Error control and recovery procedures on a message basis can be built into the network.
- A message-switching network can carry out speed and code conversion. Two

stations of different data rates can be connected since each connects to its node at its proper data rate. The message-switching network can also easily convert format (e.g. from ASCII to EBCDIC). These features are less often found in a circuit-switched system.

- Messages sent to inoperative terminals may be intercepted and either stored or rerouted to other terminals.

The primary disadvantage of message switching is that it is not suited to real-time or interactive traffic. The delay through the network is relatively long and has relatively high variance. Thus it cannot be used for voice connections. Nor is it suited to interactive terminal-host connections.

PACKET SWITCHING

Packet switching represents an attempt to combine the advantages of message and circuit switching while minimising the disadvantages of both. In situations where there is a substantial volume of traffic among a number of stations, this objective is met. Figure 3.18b illustrates the concept of packet switching.

Packet switching is very much like message switching. The principal external difference is that the length of the units of data that may be transmitted is limited in a packet-switched network. A typical maximum length is 1000 to a few thousand bits. Message switching systems accommodate far larger messages. From a station's point of view, then, messages above the maximum length must be divided into smaller units and sent out one at a time. To distinguish the two techniques, the data units in the latter system are referred to as packets.

Again using Figure 3.17 for an example, consider the transfer of a single packet. The packet contains data plus a destination address. Station A transmits the packet to 4, which stores it briefly and then passes it to 5, which passes it to 6 and on to E. One difference from message switching is that packets are typically not filed. A copy may be temporarily stored for error recovery purposes, but that is all.

On the face of it, packet switching may seem a strange procedure to adopt, with no particular advantage over message switching. Remarkably, the simple expedient of limiting the maximum size of a data unit to a rather small length has a dramatic effect on performance. Before demonstrating this, we define two common procedures for handling entire messages over a packet-switched network.

The problem is this : A station has a message to send that is of length greater than the maximum packet size. It breaks the message into packets and sends these packets to its node. Question: How will the network handle this stream of packets? There are two approaches: datagram and virtual circuit.

In the **datagram** approach, each packet is treated independently, just as each message is treated independently in a message-switched network. Let us consider the implications of this approach. Suppose that station A has a 3-packet message to send to E. It pops the packets out, 1-2-3, to node 4. On each packet, node 4 must make

a routing decision. Packet 1 comes in and node 4 determines that its queue of packets for node 5 is shorter than for node 7, so it queues the packet for node 5. Ditto for packet 2. But for packet 3, node 4 finds that its queue for node 7 is shortest and so queues packet for node 5 for that node. So the packets, each with the same destination address, do not all follow the same route. Furthermore, it is just possible that packet 3 will beat packet 2 to node 6. Thus it is possible that the packets will be delivered to E in a different sequence from the one in which they were sent. It is up to E to figure out how to reorder them. In this technique each packet, treated independently, is referred to as a "datagram".

In the **virtual circuit** approach, a logical connection is established before any packets are sent. For example, suppose that A has one or more messages to send to E. It first sends a Call Request packet to 4, requesting a connection to E. Node 4 decides to route the request and all subsequent data to 5, which decides to route the request and all subsequent data to 6, which finally delivers the Call Request packet to E. If E is prepared to accept the connection, it sends out a Call Accept packet to 6. This packet is passed back through nodes 5 and 4 to A. Stations A and E may now exchange data over the logical connection or virtual circuit that has been established. Each packet now contains a virtual circuit identifier as well as data. Each node on the pre-established route knows where to direct such packets; no routing decisions are required. Thus every data packet from A traverses nodes 4, 5 and 6; every data packet from E traverses nodes 6, 5 and 4. Eventually, one of the stations terminates the connection with a Clear Request packet. At any time, each station can have more than one virtual circuit to any other station and can have virtual circuits to more than one station.

So the main characteristic of the virtual circuit technique is that a route between stations is set up prior to data transfer. Note that this does not mean that there is a dedicated path, as in circuit switching. A packet is still buffered at each node and queued for output over a line. The difference from the datagram approach is that the node need not make a routing decision for each packet. It is made only once for each connection.

If two stations wish to exchange data over an extended period of time, there are certain advantages to virtual circuits. They all have to do with relieving the stations of unnecessary communication processing functions. A virtual circuit facility may provide a number of services, including sequencing, error control and flow control. We emphasise the word "may" because not all virtual circuit facilities will be completely reliable in providing all these services. With that proviso, we define terms. Sequencing refers to the fact that, since all packets follow the same route, they arrive in the original order. Error control is a service that assures not only that packets arrive in proper sequence, but all packets arrive correctly. For example, if a packet in a sequence fails to arrive at node 6, or arrives with an error, it can request a retransmission of that packet from node 4. Finally, flow control is a technique for assuring that a sender does not overwhelm a receiver with data. For example, if station E is buffering data from A and perceives that it is about to run out of buffer space, it can request, via the virtual circuit facility, that A suspend transmission until further notice.

One advantage of the datagram approach is that call set-up phase is avoided. Thus if a station wishes to send only one or a few packets, datagram delivery will be quicker. Another advantage of the datagram service is that, because it is more primitive, it is more flexible. A good example of this is the use of the datagram approach in inter-networking. A third advantage is that datagram delivery is inherently more reliable. If a node fails, all virtual circuits that pass through that node are lost. With datagram delivery, if a node is lost, packets may find alternate routes.

We now return to the question of performance, illustrating the techniques discussed in Figure 3.19. This figure intends to suggest the relative performance of the techniques; however, actual performance depends on a host of factors, including:

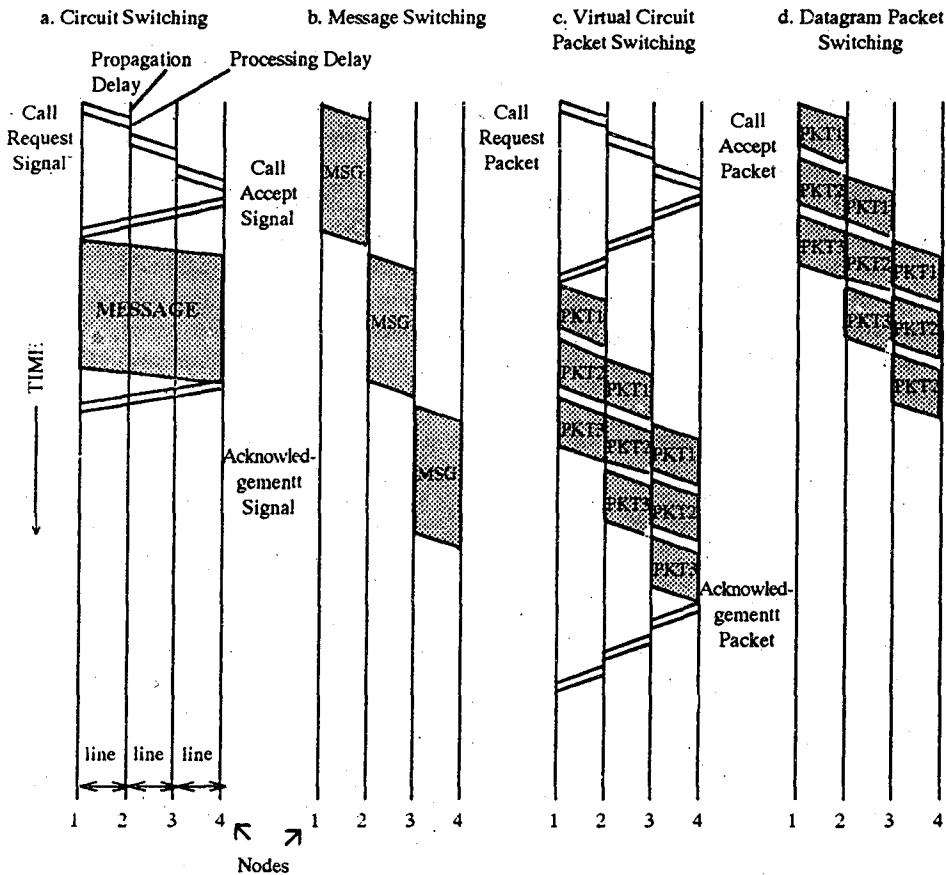


Fig. 3.19 : Even Timing for Various Communication Switching Techniques

- Number of stations
- Number and arrangement of nodes
- Total load on system
- Length (in time and data) of typical exchange between two stations

And more. Given the difficulty of comparing these methods, we hazard a few observations.

For interactive traffic, message switching is not appropriate.

For light and/or intermittent loads, circuit switching is the most cost effective, since the public telephone system can be used, via dial-up lines.

For very heavy and sustained loads between two stations, a leased circuit-switched line is the most cost effective.

Packet switching is to be preferred when there is a collection of devices that must exchange a moderate to heavy amount of data; line utilisation is most efficient with this technique.

Datagram packet switching is good for short messages and for flexibility.

Virtual circuit packet switching is good for long exchanges and for relieving stations of processing burden.

Table 3.10 summarises the main features of the four techniques that we have discussed.

TABLE 3.10 : Comparison of Communication Switching Techniques

Circuit Switching	Message Switching	Datagram Packet Switching	Virtual Circuit Packet Switching
Dedicated transmission path	No dedicated path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of messages	Transmission of packets	Transmission of packets
Fast enough for interactive	Too slow for interactive	Fast enough for interactive	Fast, enough for interactive
Messages are not stored	Messages are filed for later retrieval	Packets may be stored until delivered	Packets stored
Path is established for entire conversation	Route established for each message	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Message transmission delay	Packet transmission delay	Call setup delay; packet transmission delay
Busy signal if called party busy	No busy signal	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block	Overload increases	Overload increases	Overload may block

call setup; no delay for established calls	message delay	packet delay	call setup; increases packet delay
Electromechanical or computerized switching nodes	Message switch center with filling facility	Small switching nodes	Small switching nodes
User responsible for message-loss protection	Network responsible for messages	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth transmission	Dynamic use of bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each message	Overhead bits in each packet	Overhead bits in each packet

As a final point, we mention one common means of making packet-switched networks cost effective, and that is to provide a public connection service. Examples of such networks in the United States are TELENET and TYMNET. The network consists of nodes owned by the network service provider and linked together by leased channels from common carriers such as AT&T. Subscribers pay fees for attaching to the network and for transmitting packets through it. Whereas individual subscribers may not have sufficient traffic to make a packet-switched network economically feasible, the total demand of all subscribers justifies the network. These networks are referred to as value-added networks (VANs) because they take a basic long-haul transmission service (e.g., AT&T) and add value (the packet-switching logic). In some other countries, there is a single national-monopoly network, called a public data network (PDN). Circuit switching is a widely used switching technique for local networks. The types of networks that use this technique are the digital switch and the digital private branch exchange (PBX).

Packet switching is also commonly used for local networking. In many cases, however, there is only a single, direct path from source to destination. Thus, often, there is no routing or switching function in a local network. Packet rather than message switching is used, to facilitate the adoption of techniques preventing any source from monopolising the medium.