# INSTRUCTION MANUAL

# Computer Networks-I Lab
# (BTCS-407)


**Prepared By:**
**Er. Vivek Thapar**
**Assistant Professor (CSE)**

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

GURU NANAK DEV ENGINEERING COLLEGE
LUDHIANA - 141006

# DECLARATION

This Manual of Computer Networks-I Lab (BTCS-407) has been prepared by me as per syllabus of Computer Networks-I Lab (BTCS-407).

**Signature**

# INDEX

# 1. To Study Various Topologies for Establishing Computer Networks.

## Topologies

**1.1 Network Topology: Network topology** is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically or logically. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two networks, yet their topologies may be identical.

An example is a local area network (LAN): Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines the logical topology of the network.

**Topology**

There are two basic categories of network topologies: physical topologies and logical topologies. The shape of the cabling layout used to link devices is called the physical topology of the network. This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits. The logical topology in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology. For example, the original twisted pair Ethernet using repeater hubs was a logical bus topology with a physical star topology layout. Token Ring is a logical ring topology, but is wired a physical star from the Media Access Unit.

The logical classification of network topologies generally follows the same classifications as those in the physical classifications of network topologies but describes the path that the data takes between nodes being used as opposed to the actual physical connections between nodes. The logical topologies are generally determined by network protocols as opposed to being determined by the physical layout of cables, wires, and network devices or by the flow of the electrical signals, although in many cases the paths that the electrical signals take between nodes may closely match the logical flow of data, hence the convention of using the terms logical topology and signal topology interchangeably.

Logical topologies are often closely associated with Media Access Control methods and protocols. Logical topologies are able to be dynamically reconfigured by special types of equipment such as routers and switches.

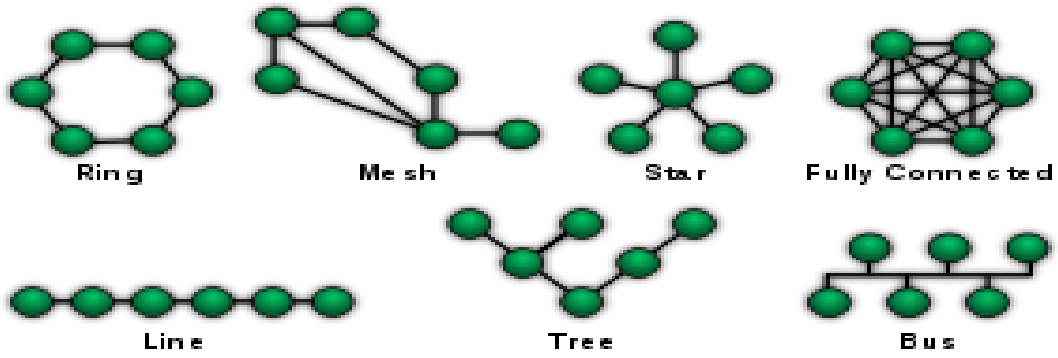



**Fig. 1.1 Diagram of Different Network Topologies**.

The study of network topology recognizes eight basic topologies: point-to-point, bus, star, ring or circular, mesh, tree, hybrid, or daisy chain.

### 1.2 Point-to-Point

The simplest topology with a permanent link between two endpoints. Switched point-to-point topologies are the basic model of conventional telephony. The value of a permanent point-to-point network is unimpeded communications between the two endpoints. The value of an on-demand point-to-point connection is proportional to the number of potential pairs of subscribers and has been expressed as Metcalfe's Law.

**Permanent (dedicated)**

Easiest to understand, of the variations of point-to-point topology, is a point-to-point communications channel that appears, to the user, to be permanently associated with the two endpoints. A children's tin can telephone is one example of a physical dedicated channel.

Within many switched telecommunications systems, it is possible to establish a permanent circuit. One example might be a telephone in the lobby of a public building, which is programmed to ring only the number of a telephone dispatcher. "Nailing down" a switched connection saves the cost of running a physical circuit between the two points. The resources in such a connection can be released when no longer needed, for example, a television circuit from a parade route back to the studio.

**Switched:**

Using circuit-switching or packet-switching technologies, a point-to-point circuit can be set up dynamically and dropped when no longer needed. This is the basic mode of conventional telephony.

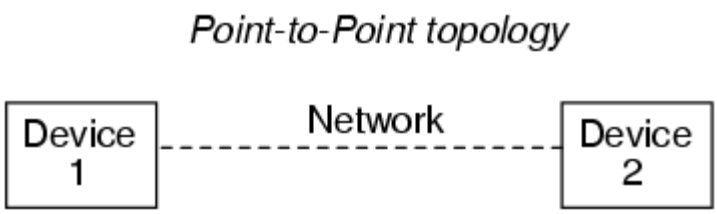
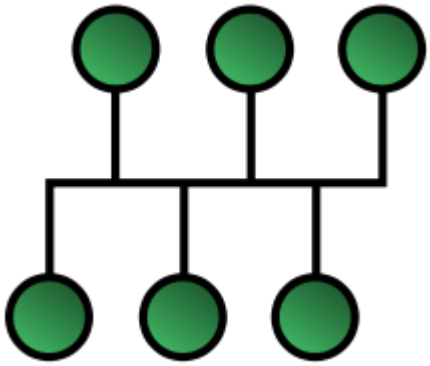



**Fig.1.2 Point to Point Network Topology**

**1.3 Bus**

Bus network



**1.3 Bus Network Topology**

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

**Linear bus**

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

**Note:** When the electrical signal reaches the end of the bus, the signal "echoes" back down the line, causing unwanted interference. As a solution, the two endpoints of the bus are normally terminated with a device called a terminator that prevents this echo.

**Distributed bus**

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

## 1.4 Star

Star network

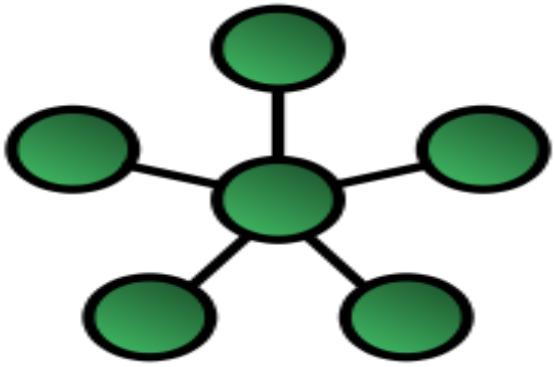


**Fig 1.4 Star Network Topology**

In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch. The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device. All traffic that traverses the network passes through the central hub. The hub acts as a signal repeater. The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the hub represents a single point of failure.

**Extended star**

A type of network topology in which a network that is based upon the physical star topology has one or more repeaters between the central node (the 'hub' of the star) and the peripheral or 'spoke' nodes, the repeaters being used to extend the maximum transmission distance of the point-to-point links between the central node and the peripheral nodes beyond that which is supported by the transmitter power of the central node or beyond that which is supported by the standard upon which the physical layer of the physical star network is based.

If the repeaters in a network that is based upon the physical extended star topology are replaced with hubs or switches, then a hybrid network topology is created that is referred to as a physical hierarchical star topology, although some texts make no distinction between the two topologies.

**Distributed Star**

A type of network topology that is composed of individual networks that are based upon the physical star topology connected in a linear fashion – i.e., 'daisy-chained' – with no central or top level connection point (e.g., two or more 'stacked' hubs, along with their associated star connected nodes or 'spokes').

## 1.5 Ring

Ring network

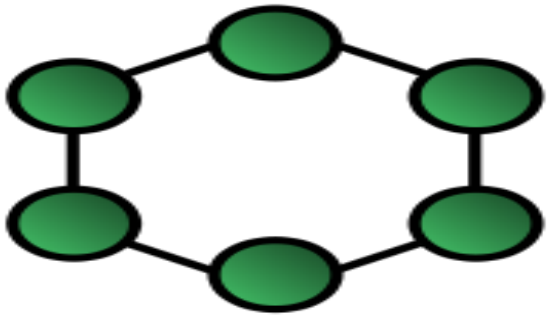


**Fig 1.5 Ring Network Topology**

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring. The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. In a ring topology, there is no server computer present; all nodes work as a server and repeat the signal. The disadvantage of this topology is that if one node stops working, the entire network is affected or stops working.

## 1.6 Mesh

Mesh networking

The value of fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

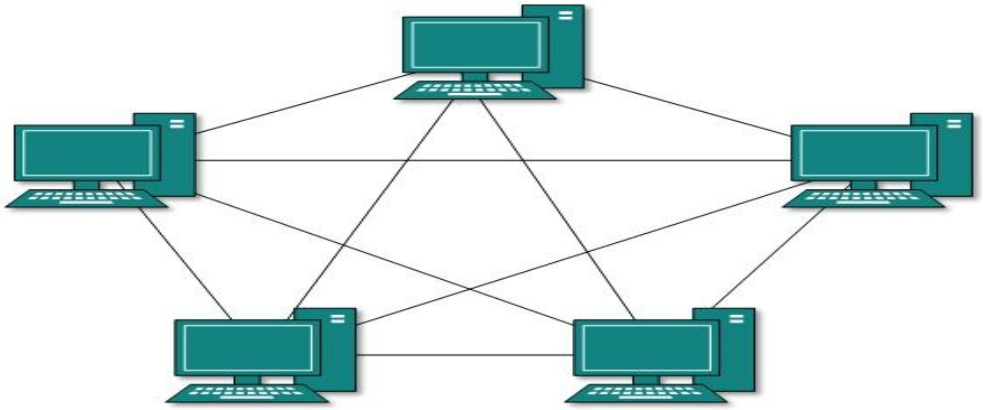


**Fig 1.6 Mesh Network Topology**

### 1.7 Fully Connected network

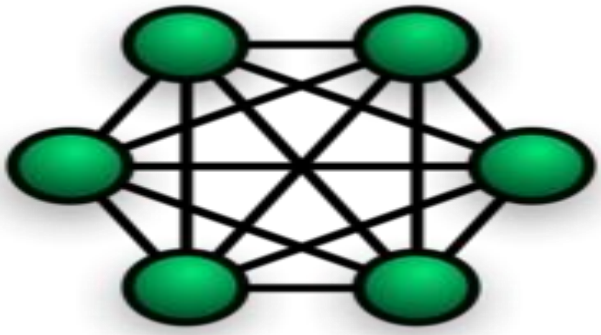


**Fig 1.7 Fully Connected Mesh Topology**

A **fully connected network** is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, as per the formula

$$c = \frac{n(n-1)}{2}.$$

and so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

### 1.8 Partially Connected

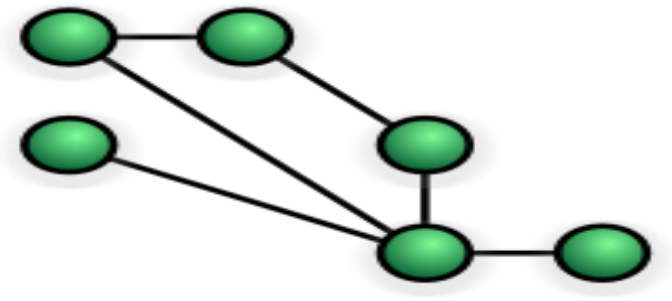


**Fig 1.8 Partially Connected Mesh Topology**

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

Tree topology is structured like a tree in real world. Tree structure has a root node, intermediate nodes and leaves. Root node is the main or head node of the structure, and the leaves are the last nodes, which has no further child nodes. This structure is arranged in a hierarchical form, any nodes can have any number of the child nodes. But the tree topology is practically impossible to construct, because the node in the network is nothing, but the computing device can have maximum one or two connections, so we cannot attach more than 2 child nodes to the computing device (or parent node). There are many sub structures under tree topology, but the most convenient is B-tree topology whereby finding errors is relatively easy.

1. A network that is based upon the physical hierarchical topology must have at least three levels in the hierarchy of the tree, since a network with a central 'root' node and only one hierarchical level below it would exhibit the physical topology of a star.
2. A network that is based upon the physical hierarchical topology and with a branching factor of 1 would be classified as a physical linear topology.
3. The branching factor, f, is independent of the total number of nodes in the network and, therefore, if the nodes in the network require ports for connection to other nodes the total number of ports per node may be kept low even though the total number of nodes is large; – this makes the effect of the cost of adding ports to each node totally dependent upon the branching factor and may therefore be kept as low as required without any effect upon the total number of nodes that are possible.
4. The total number of point-to-point links in a network that is based upon the physical hierarchical topology will be one less than the total number of nodes in the network.

5. If the nodes in a network that is based upon the physical hierarchical topology are required to perform any processing upon the data that is transmitted between nodes in the network, the nodes that are at higher levels in the hierarchy will be required to perform more processing operations on behalf of other nodes than the nodes that are lower in the hierarchy. Such a type of network topology is very useful and highly recommended.

**Advantages**

- **It is scalable.** Secondary nodes allow more devices to be connected to a central node.
- Point to point connection of devices.
- Having different levels of the network makes it more manageable hence easier fault identification and isolation.

An example of this network could be cable TV technology. Other examples are in dynamic tree based wireless networks for military, mining and otherwise mobile applications

**Disadvantages**

- Maintenance of the network may be an issue when the network spans a great area.
- Since it is a variation of bus topology, if the backbone fails, the entire network is crippled.

An example of this network could be cable TV technology. Other examples are in dynamic tree based wireless networks for military, mining and otherwise mobile applications. The Naval Postgraduate School, Monterey CA, demonstrated such tree based wireless networks for border security. In a pilot system, aerial cameras kept aloft by balloons relayed real time high resolution video to ground personnel via a dynamic self healing tree based network.

**1.9 Hybrid**

Hybrid networks use a combination of any two or more topologies, in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example a tree network connected to a tree network is still a tree network topology. A hybrid topology is always produced when two different basic network topologies are connected. Two common examples for Hybrid network are: star ring network and star bus network

- A Star ring network consists of two or more star topologies connected using a multi station access unit (MAU) as a centralized hub.
- A Star Bus network consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone).

While grid and tours networks have found popularity in high-performance computing applications, some systems have used genetic algorithms to design custom networks that have the fewest possible hops in between different nodes. Some of the resulting layouts are nearly incomprehensible, although they function quite well. A Snowflake topology is really a "Star of Stars" network, so it exhibits characteristics of a hybrid network topology but is not composed of two different basic network topologies being connected.

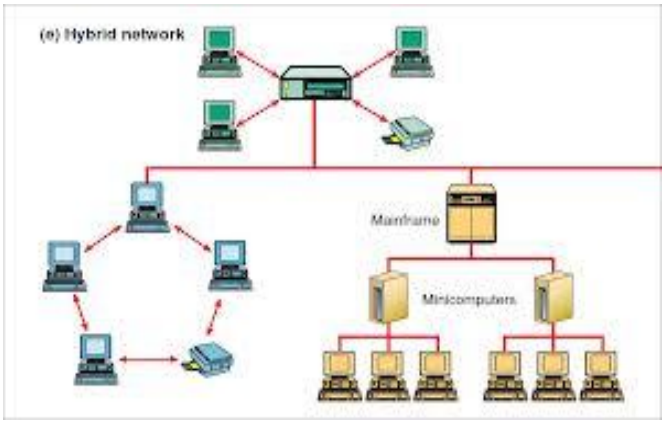



**Fig 1.9 Hybrid Network Topology**

### 1.10 Daisy chain

Except for star-based networks, the easiest way to add more computers into a network is by daisy-chaining, or connecting each computer in series to the next. If a message is intended for a computer partway down the line, each system bounces it along in sequence until it reaches the destination. A daisy-chained network can take two basic forms: linear and ring.

- A **linear topology** puts a two-way link between one computer and the next. However, this was expensive in the early days of computing, since each computer (except for the ones at each end) required two receivers and two transmitters.
- By connecting the computers at each end, a ring topology can be formed. An advantage of the ring is that the number of transmitters and receivers can be cut in half, since a message will eventually loop all of the way around. When a node sends a message, the message is processed by each computer in the ring. If the ring breaks at a particular link then the transmission can be sent via the reverse path thereby ensuring that all nodes are always connected in the case of a single failure.

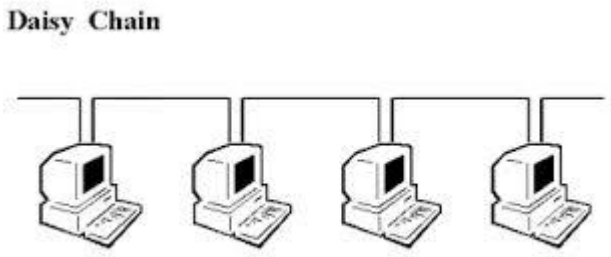



**Fig 1.10 Daisy Chain Network Topology**

## 1.11 Centralization

The star topology reduces the probability of a network failure by connecting all of the peripheral nodes (computers, etc.) to a central node. When the physical star topology is applied to a logical bus network such as Ethernet, this central node (traditionally a hub) rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, sometimes including the originating node. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. The failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the remaining peripheral nodes will be unaffected. However, the disadvantage is that the failure of the central node will cause the failure of all of the peripheral nodes. If the central node is passive, the originating node must be able to tolerate the reception of an echo of its own transmission, delayed by the two-way round trip transmission time (i.e. to and from the central node) plus any delay generated in the central node. An active star network has an active central node that usually has the means to prevent echo-related problems.

A **tree topology** (hierarchical topology) can be viewed as a collection of star networks arranged in a hierarchy. This tree has individual peripheral nodes (e.g. leaves) which are required to transmit to and receive from one other node only and are not required to act as repeaters or regenerators. Unlike the star network, the functionality of the central node may be distributed. As in the conventional star network, individual nodes may thus still be isolated from the network by a single-point failure of a transmission path to the node. If a link connecting a leaf fails, that leaf is isolated; if a connection to a non-leaf node fails, an entire section of the network becomes isolated from the rest. To alleviate the amount of network traffic that comes from broadcasting all signals to all nodes, more advanced central nodes were developed that are able to keep track of the identities of the nodes that are connected to the network. These network switches will "learn" the layout of the network by "listening" on each port during normal data transmission, examining the data packets and recording the address/identifier of each connected node and which port it is connected to in a lookup table held in memory. This lookup table then allows future transmissions to be forwarded to the intended destination only.

### 1.12 Decentralization

In a mesh topology (i.e., a partially connected mesh topology), there are at least two nodes with two or more paths between them to provide redundant paths to be used in case the link providing one of the paths fails. This decentralization is often used to compensate for the single-point-failure disadvantage that is present when using a single device as a central node (e.g., in star and tree networks). A special kind of mesh, limiting the number of hops between two nodes, is a hypercube. The number of arbitrary forks in mesh networks makes them more difficult to design and implement, but their decentralized nature makes them very useful. In 2012 the IEEE published the shortest path bridging protocol to eases configuration tasks and allows all paths to be active which increases bandwidth and redundancy between all devices. This is similar in some ways to a grid network, where a linear or ring topology is used to connect systems in multiple directions.

A fully connected network, complete topology, or full mesh topology is a network topology in which there is a direct link between all pairs of nodes. In a fully connected network with n nodes, there are n(n-1)/2 direct links. Networks designed with this topology are usually very expensive to set up, but provide a high degree of reliability due to the multiple paths for data that are provided by the large number of redundant links between nodes. This topology is mostly seen in military applications.

# 2. To Learn the Usage of Various Basic Tools (crimping, krone etc.) used in Establishing a LAN.

### 2.1 Crimping Tool

A crimping tool is a tool designed to crimp or connect a connector to the end of a cable. For example, network cables and phone cables are created using a crimping tool to connect the RJ-45 and RJ-11 connectors to the end of the cable. In the example picture below, this crimper is capable of crimping a RJ-11 (6-Pin) and RJ-45 (8-Pin) connectors and also includes a wire cutter near the handles that can be used to cut phone or CAT5 cable.

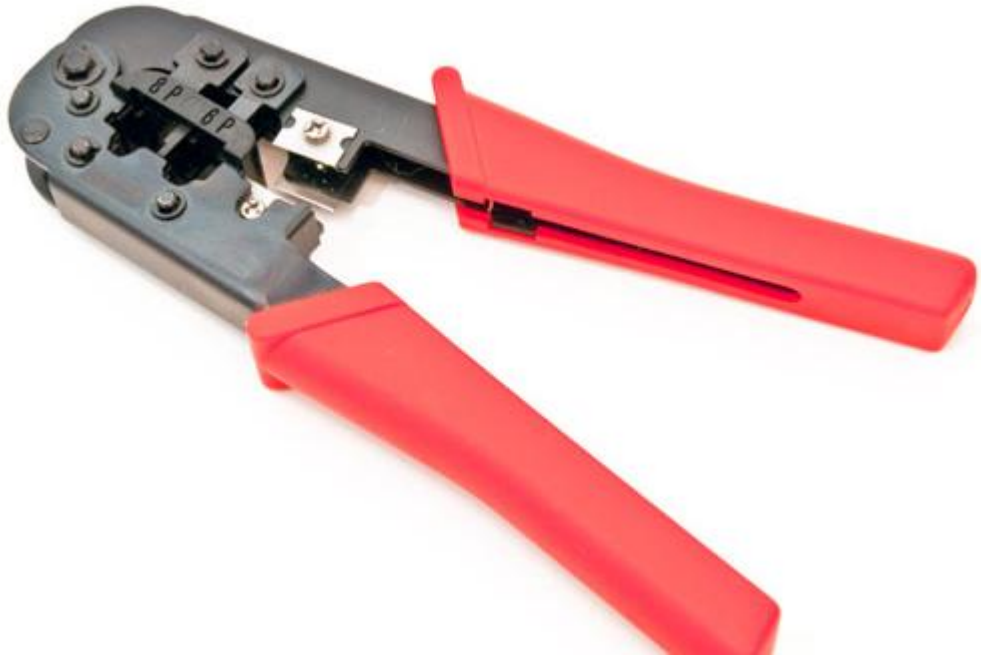



**Fig. 2.1 Crimping Tool**

To use this crimping tool, each wire is first placed into the connector. Once all the wires are in the jack, the connectors with wires are placed into the crimping tool, and the handles are squeezed together. Crimping makes the plastic connector puncture and hold each of the wires, which prevents the wires from falling out and for data to be transmitted from the connector to each of the wires.

### 2.2 Krone Tool

A punch down tool, also called a punch down tool or a krone tool (named after the KRONE LSA-PLUS connector), is a small hand tool used by telecommunication and network technicians. It is used for inserting wire into insulation-displacement connectors on punch down blocks, patch panels, keystone modules, and surface mount boxes (also known as biscuit jacks).

**Fig. 2.2 Krone Tool**

Most punch down tools are of the impact type, consisting of a handle, an internal spring mechanism, and a removable slotted blade. To use the punch down tool, a wire is pre-positioned into a slotted post on a punch block, and then the punch down tool is pressed down on top of the wire, over the post. Once the required pressure is reached, an internal spring is triggered, and the blade pushes the wire into the slot, simultaneously cutting the insulation and securing the wire. The tool blade does not cut throughout the wire insulation to make contact, but rather the sharp edges of the slot in the contact post itself slice through the insulation.

However, the punch down tool blade also is usually used to cut off excess wire, in the same operation as making the connection; this is done with a sharp edge of the punch down tool blade trapping the wire to be cut against the plastic punch block. If this cutoff feature is heavily used, the tool blade must be re sharpened or replaced from time to time. Tool blades without the sharp edge are also available; these are used for continuing a wire through a slotted post to make connections with another slotted post ("daisy-chained" wiring).

For light-duty use, there are also less-expensive punch down tools with fixed blades and no impact mechanism. These low-cost tools are more time-consuming for making reliable connections, and can cause muscle fatigue when used for large numbers of connections.

To accommodate different connector types, 66, 110, BIX and krone blocks require different blades. Removable blades for 66 or 110 are almost always double-ended. Some blades have one end that only inserts the wire for daisy-chain wiring from post to post, and another end that inserts wire and trims the excess length for termination at a post. Other blades have a cutting 66 blade on one end and a cutting 110 blade on the other. Krone blades require a separate scissor-like mechanism for trimming the wire.

# 3. To Familiarize with Switch and Hub used in Networks.

### 3.1 Switch

A network switch (sometimes known as a switching hub) is a computer networking device that is used to connect devices together on a computer network, by using a form of packet switching to forward data to the destination device. A network switch is considered more advanced than a hub because a switch will only forward a message to one or multiple devices that need to receive it, rather than broadcasting the same message out of each of its ports.

A network switch is a multi-port network bridge that processes and forwards data at the data link layer (layer 2) of the OSI model. Switches can also incorporate routing in addition to bridging. Switches may operate at one or more layers of the OSI model, including the data link and network layers. A device that operates simultaneously at more than one of these layers is known as a multilayer switch.

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fiber Channel, ATM, ITU-T and 802.11. This connectivity can be at any of the layers mentioned. While layer-2 functionality is adequate for bandwidth-shifting within one technology, interconnecting technologies such as Ethernet and token ring is easier at layer 3.

Devices that interconnect at layer 3 are traditionally called routers, so layer-3 switches can also be regarded as (relatively primitive) routers.

Where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules. Some vendors provide firewall, network intrusion detection and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.

In other cases, the switch is used to create a mirror image of data that can go to an external device. Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet .Switches may operate at one or more layers of the OSI model, including the data link and network layers. A device that operates simultaneously at more than one of these layers is known as a multilayer switch.

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fibre Channel, ATM, ITU-T G.hn and 802.11. This connectivity can be at any of the layers mentioned. While layer-2 functionality is adequate for bandwidth-shifting within one technology, interconnecting technologies such as Ethernet and token ring is easier at layer 3.

Devices that interconnect at layer 3 are traditionally called routers, so layer-3 switches can also be regarded as (relatively primitive) routers.

Where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules. Some vendors provide firewall,[4][5] network intrusion detection,[6] and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.[7]

In other cases, the switch is used to create a mirror image of data that can go to an external device. Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet sniffers.Sniffers es are commonly known as layer-3 or multilayer switches. Switches exist for various types of networks including Fiber Channel, Asynchronous Transfer Mode, Infini Band, Ethernet and others

**Fig. 3.1 Switch**

A switch is a device used on a computer network to physically connect devices together. Multiple cables can be connected to a switch to enable networked devices to communicate with each other. Switches manage the flow of data across a network by only transmitting a received message to the device for which the message was intended. Each networked device connected to a switch can be identified using a MAC address, allowing the switch to regulate the flow of traffic. This maximizes security and efficiency of the network.

Because of these features, a switch is often considered more "intelligent" than a network hub. Hubs neither provide security, or identification of connected devices. This means that messages have to be transmitted out of every port of the hub, greatly degrading the efficiency of the network.

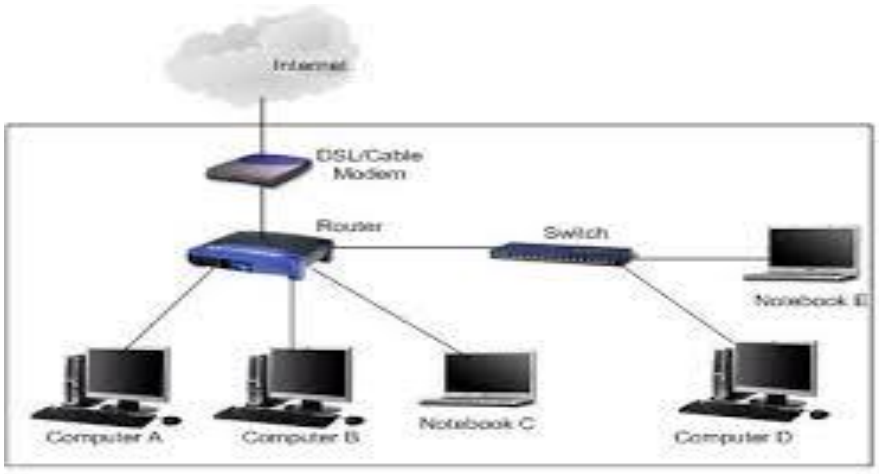



**Fig. 3.2 Use of Switch**

An Ethernet switch operates at the data link layer of the OSI model to create a separate collision domain for each switch port. With four computers (e.g., A, B, C and D) on four switch ports, any pair (e.g. A and B) can transfer data back and forth while the other pair (e.g. C and D) also do so simultaneously, and the two conversations will not interfere with one another. In full duplex mode, these pairs can also overlap (e.g. A transmits to B, simultaneously B to C, and so on). In the case of using a repeater hub, they would all share the bandwidth and run in half duplex, resulting in collisions which would require retransmissions.

The network switch plays an integral part in most modern Ethernet local area networks (LANs). Mid-to-large sized LANs contain a number of linked managed switches. Small office/home office (SOHO) applications typically use a single switch, or an all-purpose converged device such as a residential gateway to access small office/home broadband services such as DSL or cable Internet. In most of these cases, the end-user device contains a router and components that interface to the particular physical broadband technology. User devices may also include a telephone interface for VoIP.Segmentation is the use of a bridge or a switch (or a router) to split a larger collision domain into smaller ones in order to reduce collision probability and improve overall throughput. In the extreme, i. e. micro segmentation, each device is located on a dedicated switch port. In contrast to an Ethernet hub, there is a separate collision domain on each of the switch ports. This allows computers to have dedicated bandwidth on point-to-point connections to the network and also to run in full-duplex without collisions. Full-duplex mode has only one transmitter and one receiver per 'collision domain', making collisions impossible.

### 3.2 Role of switches in a network

Switches may operate at one or more layers of the OSI model, including the data link and network layers. A device that operates simultaneously at more than one of these layers is known as a multilayer switch.

In switches intended for commercial use, built-in or modular interfaces make it possible to connect different types of networks, including Ethernet, Fibre Channel, ATM, ITU-T and 802.11. This connectivity can be at any of the layers mentioned. While layer-2 functionality is adequate for bandwidth-shifting within one technology, interconnecting technologies such as Ethernet and token ring is easier at layer 3.

Devices that interconnect at layer 3 are traditionally called routers, so layer-3 switches can also be regarded as (relatively primitive) routers.

Where there is a need for a great deal of analysis of network performance and security, switches may be connected between WAN routers as places for analytic modules. Some vendors provide firewall, network intrusion detection and performance analysis modules that can plug into switch ports. Some of these functions may be on combined modules.

In other cases, the switch is used to create a mirror image of data that can go to an external device. Since most switch port mirroring provides only one mirrored stream, network hubs can be useful for fanning out data to several read-only analyzers, such as intrusion detection systems and packet sniffers.

### 3.3 Hubs

Networking hubs are central components of local area networks (LANs). To understand the role of networking hubs, a basic understanding of LANs is required. Whenever one or more computers are networked together, a LAN is created. A LAN can be vital at work, but it can also be useful at home. The purpose of joining computers together in a LAN is to share resources like files, a printer, a scanner, or Internet access.

There are four components in a basic wired hub network:

**Ethernet wire**: This is the physical cable that links the computers together, enabling them to talk to each other. The Ethernet cable, also called twisted pair, *or* 10-Base T, plugs into a network card located in each computer on the LAN.

**Network** Interface **Cards (NICs)** : One of these cards goes into a vacant slot inside each computer. The back of the card features a port for one end of an Ethernet cable. Newer computers normally have a networking card built-in.

**Networking Hubs**: The networking hub is a junction box with several ports in the back for receiving the Ethernet cables that are plugged into each computer on the LAN. With Ethernet cables going from each NIC to the hub, all computers are connected to the hub.

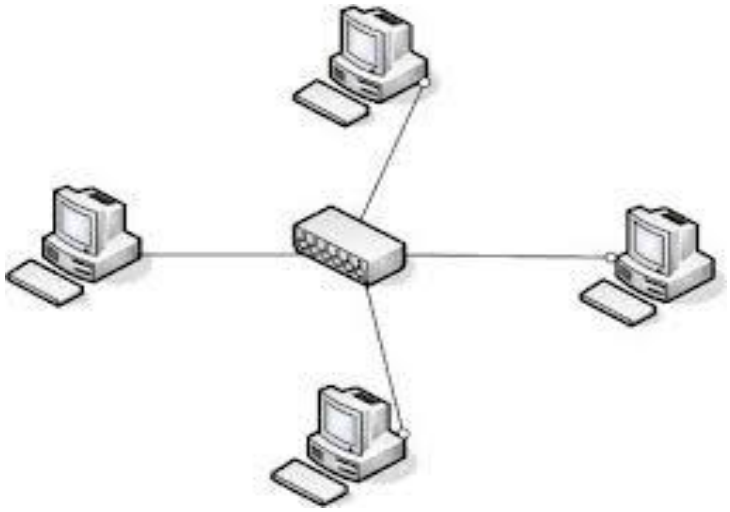


**Fig. 3.3 Use of Hub**

**3.4 What is Hub** A Hub is a networking device which receives signal from the source, amplifies it and send it to multiple destinations or computers. If you ever some across subject 'Computer Networking' then you must heard this word. Sometimes, hubs are also called Ethernet Hub, Repeater Hub, Active Hub and Network Hub. Basically it is a networking device which is used multiple devices like Computers, Servers etc to each other and make them work as a single network segment.
Hubs are used in 'Physical Layer' of OSI Model.

**3.5 Construction of Hub**
Practically Hubs is a **small box** in rectangular shape which have multiple ports for connecting various devices to it. It receives its power supply from auxiliary power sources. The main work of Hub is to receive incoming data signals, amplify them in the form of electrical signals and then send them to each connected device. A Hub may contain a number of ports. Minimum amount of ports that a hub can have is 4 and it can have up to 24 ports for connecting various devices and peripherals to it. Recommended For You: Client Server Networking Model

**3.6 Types of Hub** On the basis of its working methods, the Hubs can be divided into three types, given as:

- Active Hub
- Passive Hub
- Intelligent Hub

**Active Hub**: As its name suggests, Active Hub is a hub which can amplify or regenerate the information signal. This type of bus has an advantage as it also amplifies the incoming signal as well as forward it to multiple devices. This Bus is also known as Multiport Repeater. It can upgrade the properties if incoming signal before sending them to destination.

**Passive Hub**: Passive Hub works like a simple Bridge. It is used for just creating a connection between various devices. It does not have the ability to amplify or regenerate any incoming signal. It receives signal and then forward it to multiple devices.

**Intelligent Hub**: This is the third and last type of Bus. It can perform tasks of both Active and Passive buses. Also, it can perform some other tasks like Bridging and routing. It increases the speed and effectiveness of total network thus makes the performance of whole network fast and efficient.

**3.7 Applications Of Hub** Networking Hub is widely used networking connectivity device. It has many advantages over other connectivity devices. Some Application of Networking Hub are given below:

- Hubs are used to create small Home Networks.
- Hubs are used for monitoring the networks.
- Hubs are used in Organizations and Computer Labs for connectivity.
- It makes one device or peripheral available throughout the whole network.

# 4. To Learn the Usage of Connecters and Cables (cabling standards) used in Networks

### 4.1 Cabling and Connectors

**Cable** is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides
- Wireless LANs
- Unshielded Twisted Pair (UTP) Cable

### 4.2 Twisted Pair Cables

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

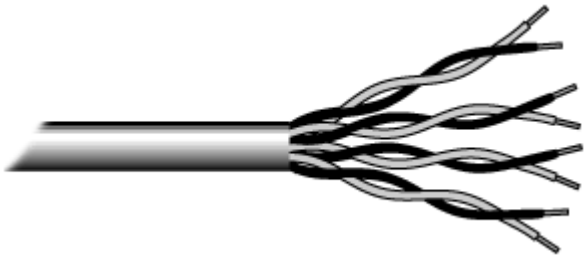


**Fig..4.1 Unshielded Twisted pair**

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported **transmission** rate and the greater the cost per foot. The EIA/TIA (Electronic Industry

Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

| Category | Speed | Use |
|---|---|---|
| 1 | 1 Mbps | Voice Only (Telephone Wire) |
| 2 | 4 Mbps | LocalTalk & Telephone (Rarely used) |
| 3 | 16 Mbps | 10BaseT Ethernet |
| 4 | 20 Mbps | Token Ring (Rarely used) |
| 5 | 100 Mbps (2 pair) | 100BaseT Ethernet |
| | 1000 Mbps (4 pair) | Gigabit Ethernet |
| 5e | 1,000 Mbps | Gigabit Ethernet |
| 6 | 10,000 Mbps | Gigabit Ethernet |

**Table 4.1 Categories of UTP Cables**

### 4.3 Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A **slot** allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

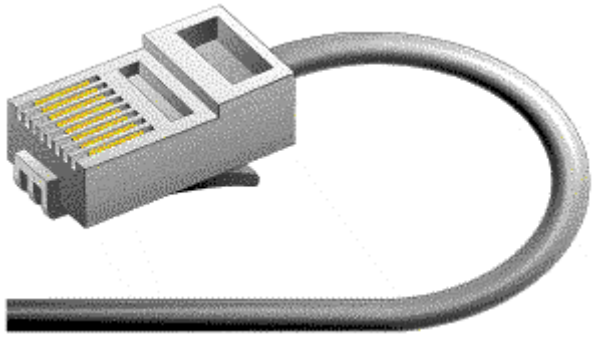


**Fig. 4.2 RJ-45 Connector**

### 4.4 Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to

the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

1. Each pair of wires is individually shielded with foil.
2. There is a foil or braid shield inside the jacket covering all wires (as a group).
3. There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

### 4.5 Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

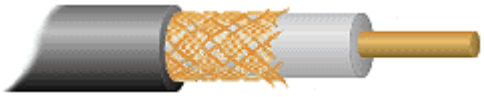


**Fig. 4.3 Coaxial Cable**

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

### 4.6 Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

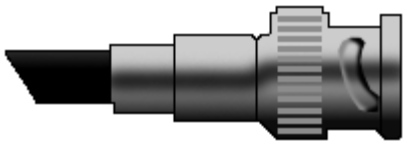


**Fig. 4.4 BNC Connector**

### 4.7 Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

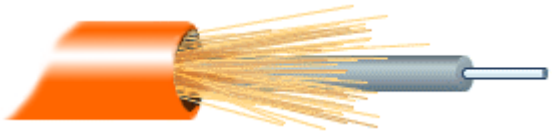


**Fig. 4.5 Fiber Optic Cable**

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

### 4.8 Fiber Optic Cable Connectors

An optical fiber connector terminates the end of an optical fiber, and enables quicker connection and disconnection than splicing. The connectors mechanically couple and align the cores of fibers so light can pass. Better connectors lose very little light due to reflection or misalignment of the fibers. In all, about 100 fiber optic connectors have been introduced to the market. Optical fiber connectors are used to join optical fibers where a connect/disconnect capability is required. The basic connector unit is a connector assembly. A connector assembly consists of an adapter and two connector plugs. Due to the polishing and tuning procedures that may be incorporated into optical connector manufacturing, connectors are generally assembled onto optical fiber in a supplier's manufacturing facility. However, the assembly and polishing operations involved can be performed in the field, for example, to make cross-connect jumpers to size. Optical fiber connectors are used in telephone company central offices, at installations on customer premises, and in outside plant applications to connect equipment and cables, or to cross-connect cables.

Most optical fiber connectors are spring-loaded, so the fiber faces are pressed together when the connectors are mated. The resulting glass-to-glass or plastic-to-plastic contact eliminates signal losses that would be caused by an air gap between the joined fibers.

**E-2000**

**Escon**

**FC**

**LC**

**ST**

**Fig 4.6 Few Fiber Optic Cable Connectors**

| Specification | Cable Type |
|---|---|
| **10BaseT** | Unshielded Twisted Pair |
| **10Base2** | Thin Coaxial |
| **10Base5** | Thick Coaxial |
| **100BaseT** | Unshielded Twisted Pair |
| **100BaseFX** | Fiber Optic |
| **100BaseBX** | Single mode Fiber |
| **100BaseSX** | Multimode Fiber |
| **1000BaseT** | Unshielded Twisted Pair |
| **1000BaseFX** | Fiber Optic |
| **1000BaseBX** | Single mode Fiber |
| **1000BaseSX** | Multimode Fiber |

**Table 4.1 Specifications of cables**

### 4.9 10BASET Cabling Standard

T568 A or T568 B Wiring Schemes

Based on **TIA**/EIA-568-B.1-2001, the T568A and T568B wiring schemes define the pinout, or order of connections, for wires in eight-pin modular connector plugs and jacks.The only difference between T568A and T568B is that pairs 2 and 3 (orange and green) are swapped. Both configurations wire the pins "straight through", i.e., pins 1 through 8 on one end are connected to pins 1 through 8 on the other end, and the same sets of pins are paired in both configurations: pins 1 and 2 form a pair, as do 3 and 6, 4 and 5 and 7 and 8.Cables that are terminated with differing standards on each end will not function normally, however mixing T568A-terminated patch cords with T568B-terminated horizontal cables (or the **reverse**) will not produce pinout problems in a facility, although it may slightly degrade signal quality, This effect is marginal and certainly no greater than that produced by mixing cable brands in-channel.

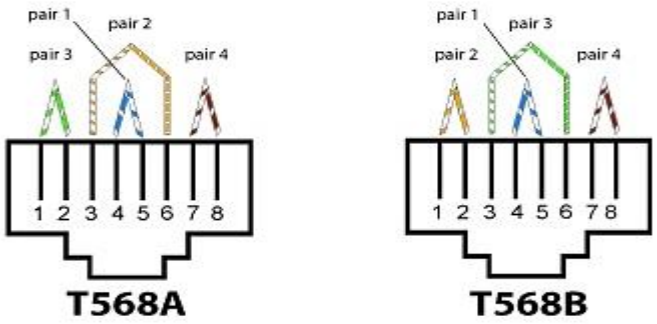



**Fig 4.7 T568A and T568B Wiring Assignments:**

| Pin # | T568B | T568A |
|---|---|---|
| 1 | White/Orange | White/Green |
| 2 | Orange | Green |
| 3 | White/Green | White/Orange |
| 4 | Blue | Blue |
| 5 | White/Blue | White/Blue |
| 6 | Green | Orange |
| 7 | White/Brown | White/Brown |
| 8 | Brown | Brown |

**Table 4.3 Wiring Standards**

### 4.10 RJ45 Color-Coded Scheme

RJ45 cables have 8 color-coded wires, and the plugs have 8 pins and conductors. Eight wires are used as 4 pairs, each representing positive and negative polarity. The most commonly used wiring standard for 100baseT is T-586B stanrard described above. Prior to EIA 568A and 568B standards, the color-coded scheme was used to wire RJ45 cables. The table below depicts pin and color schemes used in traditional and standardized setup.

| Pin | Colored Scheme | T-568B (Common) | T-568A |
|---|---|---|---|
| 1 | Blue | Orange Stripe | Green Stripe |
| 2 | Orange | Orange | Green |
| 3 | Black | Green Stripe | Orange Stripe |
| 4 | Red | Blue | Blue |
| 5 | Green | Blue Stripe | Blue Stripe |
| 6 | Yellow | Green | Orange |
| 7 | Brown | Brown Stripe | Brown Stripe |
| 8 | White (or Grey) | Brown | Brown |

**Table 4.4 Color Coding Scheme**

# 5. To Make Certain Copper and Fiber Patch Cords using Different Standards.

## 5.1 Copper Patch Cords

There are two types of copper patch cords one is **straight-through** and another one is **cross-over**.RJ-45 conductor data cable contains 4 pairs of wires each consists of a solid colored wire and a strip of the same color. There are two wiring standards for RJ-45 wiring: T-568A and T-568B. Although there are 4 pairs of wires, 10BaseT/100BaseT Ethernet uses only 2 pairs: Orange and Green. The other two colors (blue and brown) may be used for a second Ethernet line or phone connections. The two wiring standards are used to create a cross-over (T-568A on one end, and T-568B on the other end), or a straight-through cable (T-568B or T-568A on both ends).

- To create a straight-through cable, you'll have to use either T-568A or T-568B on both ends of the cable. The diagram depicted on the left and right shows clip of the RJ-45 connector down.
- To create a cross-over cable, you'll wire T-568A on one end and T-568B on the other end of the cable.

The straight-through cables are used when connecting Data Terminating Equipment (DTE) to Data Communications Equipment (DCE), such as computers and routers to modems (gateways) or hubs (Ethernet Switches). The cross-over cables are used when connecting DTE to DTE, or DCE to DCE equipment; such as computer to computer, computer to router; or gateway to hub connections. The DTE equipment terminates the signal, while DCE equipment do not.

The RJ45 data cables we use to connect computers to a Ethernet switch is straight-through cables. As noted above, the RJ45 cable uses only 2-pairs of wires: Orange (pins 1 & 2) and Green (pins 3 & 6). Pins 4, 5 (Blue) and 7, 8 (Brown) are NOT used. Straight-through cable, as its name suggests, connects pin 1 to pin 1, pin 2 to pin 2, pin 3 to pin 3, and pin 6 to pin 6. Cross-over cables are used to connect TX+ to RX+, and TX- to RX-, which connects pin 1 to pin 3, pin 2 to pin 6, pin 3 to pin 1 and pin 6 to pin 2. The unused pins are generally connected straight-through in both straight-through and cross-over cables.

To network two computers without a hub, a cross-over cable is used. Cross-over cable is also used to connect a router to a computer, or Ethernet switch (hub) to another Ethernet switch without an uplink. Most Ethernet switches today provide an uplink port, which prevents a use of cross-over cable to daisy chain another Ethernet switch. Straight-through cables are used to connect a computer to an Ethernet switch, or a router to an Ethernet switch.

There are pin number designations for each color in T-568B and T-568A.

| | T-568B | | T-568A | |
|---|---|---|---|---|
| Pin | Color | Pin Name | Color | Pin Name |
| 1 | Orange Stripe | Tx+ | Green Stripe | Rx+ |
| 2 | Orange | Tx- | Green | Rx- |
| 3 | Green Stripe | Rx+ | Orange Stripe | Tx+ |
| 4 | Blue | Not Used | Blue | Not Used |
| 5 | Blue Stripe | Not Used | Blue Stripe | Not Used |
| 6 | Green | Rx- | Orange | Tx- |
| 7 | Brown Stripe | Not Used | Brown Stripe | Not Used |
| 8 | Brown | Not Used | Brown | Not Used |

**Table 5.1 Pin Number Designations**

### 5.2 RJ45 Color-Coded Scheme

RJ45 cables have 8 color-coded wires, and the plugs have 8 pins and conductors. Eight wires are used as 4 pairs, each representing positive and negative polarity. The most commonly used wiring standard for 100baseT is T-586B stanrard described above. Prior to EIA 568A and 568B standards, the color-coded scheme was used to wire RJ45 cables. The table below depicts pin and color schemes used in traditional and standardized setup.

| Pin | Colored Scheme | T-568B (Common) | T-568A |
|---|---|---|---|
| 1 | Blue | Orange Stripe | Green Stripe |
| 2 | Orange | Orange | Green |
| 3 | Black | Green Stripe | Orange Stripe |
| 4 | Red | Blue | Blue |
| 5 | Green | Blue Stripe | Blue Stripe |
| 6 | Yellow | Green | Orange |
| 7 | Brown | Brown Stripe | Brown Stripe |
| 8 | White (or Grey) | Brown | Brown |

**Table 5.2 RJ-45 Color Coded Scheme**

### 5.3 How to Make Straight-Through Cable

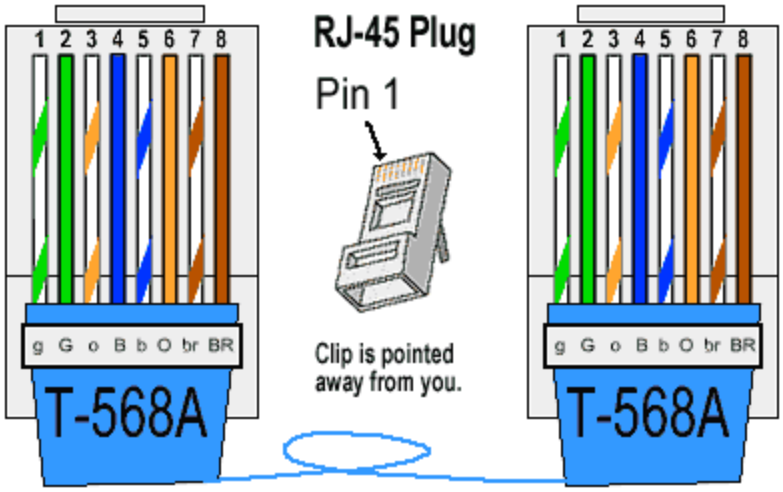
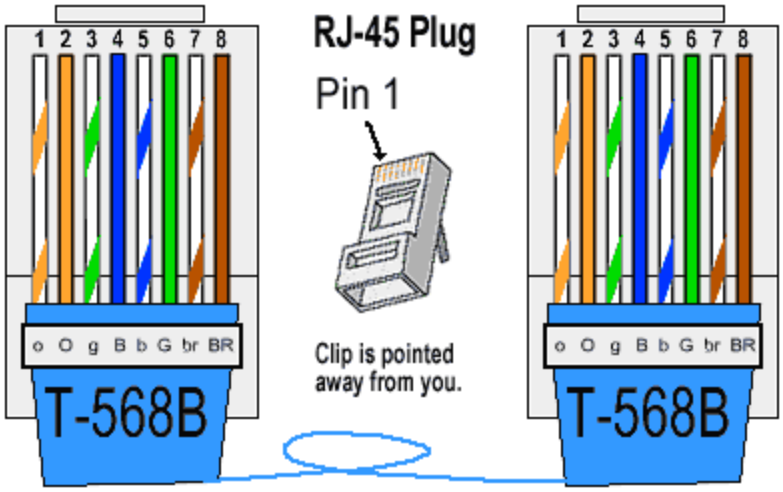



**Fig.5.1 T-568A Straight-Through Ethernet Cable**

**Or**

**T-568B Straight-Through Ethernet Cable**




Both the T-568A and the T-568B standard Straight-Through cables are used most often as patch cords for your Ethernet connections. If you require a cable to connect two

Ethernet devices directly together without a hub or when you connect two hubs together, you will need to use a Crossover cable instead.

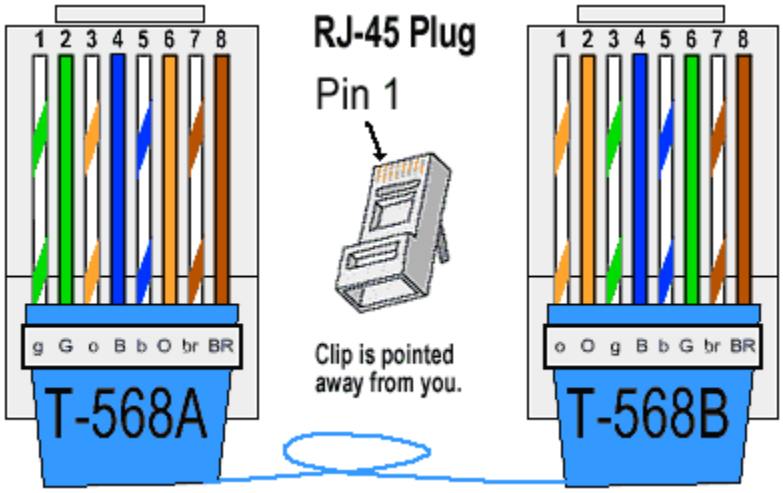



**Fig 5.2 RJ-45 Crossover Ethernet Cable**

A good way of remembering how to wire a Crossover Ethernet cable is to wire one end using the T-568A standard and the other end using the T-568B standard. Another way of remembering the color coding is to simply switch the Green set of wires in place with the Orange set of wires. Specifically, switch the solid Green (G) with the solid Orange, and switch the green/white with the orange/white.

### 5.4 Instructions for Making Cables

- Pull the cable off the reel to the desired length and cut. If you are pulling cables through holes, its easier to attach the RJ-45 plugs after the cable is pulled. The total length of wire segments between a PC and a hub or between two PC's cannot exceed 100 Meters (328 feet) for 100BASE-TX and 300 Meters for 10BASE-T.
- Start on one end and strip the cable jacket off (about 1") using a stripper or a knife. Be extra careful not to nick the wires, otherwise you will need to start over.
- Spread, untwist the pairs, and arrange the wires in the order of the desired cable end. Flatten the end between your thumb and forefinger. Trim the ends of the wires so they are even with one another, leaving only 1/2" in wire length. If it is longer than 1/2" it will be out-of-spec and susceptible to crosstalk. Flatten and insure there are no spaces between wires.
- Hold the RJ-45 plug with the clip facing down or away from you. Push the wires firmly into the plug. Inspect each wire is flat even at the front of the plug. Check the order of the wires. Double check again. Check that the jacket is fitted right

against the stop of the plug. Carefully hold the wire and firmly crimp the RJ-45 with the crimper.

- Check the color orientation, check that the crimped connection is not about to come apart, and check to see if the wires are flat against the front of the plug. If even one of these are incorrect, you will have to start over. **Test** the Ethernet cable.

### 5.5 Fiber Optic Patch Cables

Fiber optic patch cable is also known as fiber optic jumper or fiber optic patch cord. It i**s** composed of a fiber optic cable terminated with different connectors on the ends. For the fiber patch cables, there are two major application areas which are computer work station to outlet and fiber optic patch panels or optical cross connect distribution center. We provide various types of fiber patch cords including single mode, multimode, multi core, and armored versions. You can aslo find fiber optic pigtails and other special patch cables here. For most of them, the SC, ST, FC, LC, MU, MTRJ, E2000, APC/UPC connectors are all available, even we supply MPO/MTP fiber cables.

### 5. 6 Common Fiber Patch Cables

- 10G OM4 Patch Cables
- 10G OM3 Patch Cables
- Single mode Fiber Cables
- OM1 Multimode Fiber Cables
- OM2 Multimode Fiber Cables
- 100/140 Patch Cable

**Fig 5.3 Common Fiber Patch Cables**

# 6. To familiarize with Routers & Bridges

## 6.1 Routers

**Routers** are small physical devices that join multiple networks together. Technically, a router is a Layer 3 gateway device, meaning that it connects two or more networks and that the router operates at the network layer of the OSI model.

Home networks typically use a wireless or wired Internet Protocol (IP) router, IP being the most common OSI network layer protocol. An IP router such as a DSL or cable modem broadband router joins the home's local area network (LAN) to the wide-area network (WAN) of the Internet.

By maintaining configuration information in a piece of storage called the routing table, wired or wireless routers also have the ability to filter traffic, either incoming or outgoing, based on the IP addresses of senders and receivers. Some routers allow a network administrator to update the routing table from a Web browser interface. Broadband routers combine the functions of a router with those of a network switch and a firewall in a single unit.

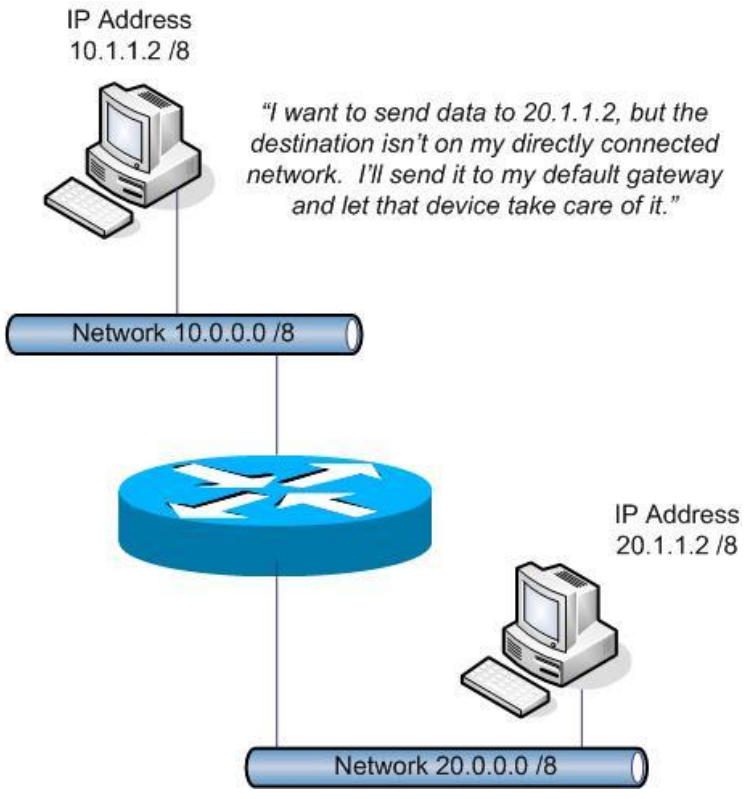



**Fig. 6.1 How Router Works**

### 6.2 How Router Works

- The router powers on and loads it's OS from flash
- The router loads the configuration file last saved to NVRAM and sets up the network interfaces and routing protocols it will run.
- The router adds the network address and subnet for each interface to it's routing table along with the name of the interface itself.
- The router has a simple static default route to send all non-local data out the network port connected to the cable company.
- When the router receives a web page request from your computer, it checks the destination IP address against its routing table.
- The bits forming the destination IP address in the IP packet are used as a hash key to point to the correct route, which in turn points to the correct network interface that the packet should be forwarded out of.
- The router transmits the packet out the correct interface, to the next router, which repeats the process until the packet reaches the destination.

### 6.3 Bridge

A bridge device filters data traffic at a network boundary. Bridges reduce the amount of traffic on a local area network (LAN) by dividing it into two segments. Bridges operate at the data link layer (Layer 2) of the OSI model. Bridges inspect incoming traffic and decide whether to forward or discard it. An Ethernet bridge, for example, inspects each incoming Ethernet frame - including the source and destination MAC addresses, and sometimes the frame size - in making individual forwarding decisions.

Bridges serve a similar function as network switches that also operate at Layer 2. Traditional bridges, though, support one network boundary (accessible through a hardware port), whereas switches usually offer four or more hardware ports. Switches are sometimes called "multi-port bridges" for this reason.

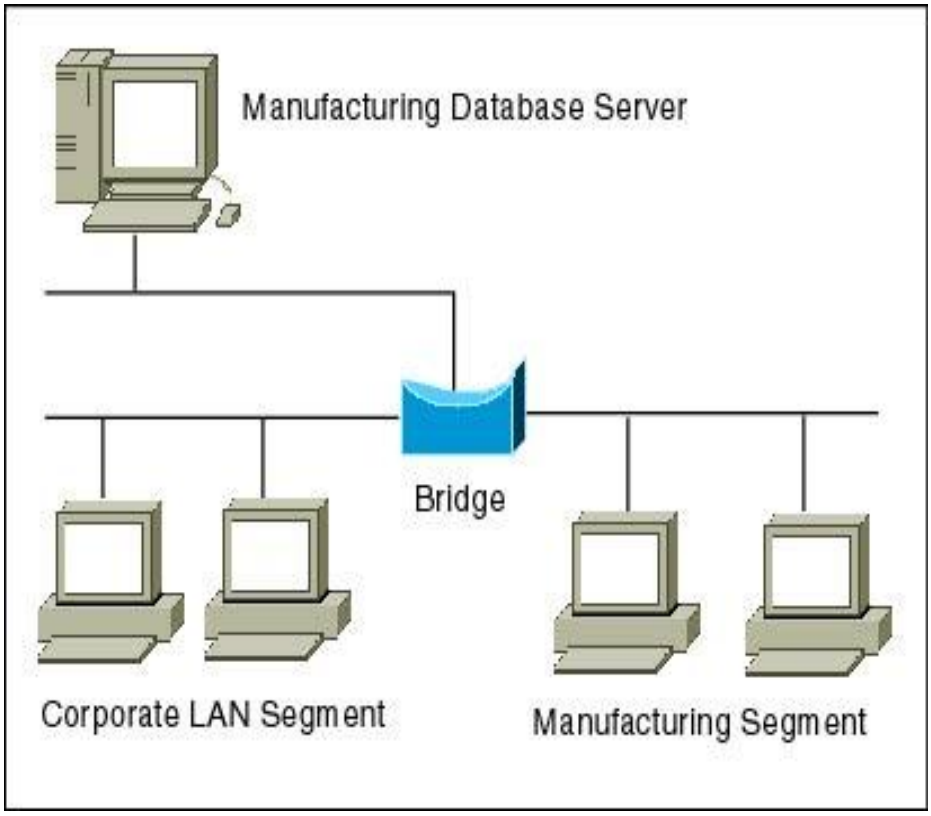



**Fig. 6.2 How Bridge Works**

The network bridge provides an inexpensive and easy way to connect local area network (LAN) segments. To understand how the network bridge works, it is important to understand what a LAN segment is. A LAN segment is a single section of network media that connects computers. For example, suppose you have three computers: computer A, computer B, and computer C. Computer A has two Ethernet network adapters, and computers B and C have one Ethernet network adapter each. An Ethernet cable connecting A to B would create one LAN segment. An additional Ethernet cable connecting A to C would create a LAN segment.

Traditionally, if you want to have a network that has more than one segment, you have two options: routing or bridging. IP routing is a common solution for connecting network segments. However, to set up for IP routing you need either to buy hardware routers or set up the computers at the junctions between segments to operate as routers. IP routing requires difficult configurations for IP addressing for each computer on each network segment, and each network segment needs to be configured as a separate subnet IP routing is a good solution for large networks, where scalability is important, and where there is an experienced staff to configure and maintain the network. A hardware bridging solution does not necessitate difficult configurations, like IP routing, but it does require that you purchase additional hardware bridges. Neither of these options are ideal if you have a home or small office network, do not want to purchase expensive bridging hardware, and do not have experienced staff to administer an IP routing network.

The network bridge, in contrast, allows you to connect LAN segments by selecting the appropriate network connection icons and clicking Bridge Connections. Similar buttons allow you to enable the bridge and add connections to it. The network bridge manages your LAN segments and creates a single subnet for the entire network. There is no configuration required, and you do not need purchase additional hardware such as routers or bridges. IP addressing, address allocation, and name resolution is highly simplified in a single subnet IP network.

The network bridge can create connections between different types of network media. In a traditional network, if you are using mixed media types you need a separate subnet for each type of media, and packet forwarding is required between each one of the network's multiple subnets. Packet forwarding is required because different protocols are used for different types of media. Network Bridge automates the configuration that is required in order to forward information from one type of media to another.

# 7. Use Commands like Ping,Ipconfig for TroubleShooting Network Related Problems.

## 7.1 PING

The Ping command is an extremely useful command line utility that can help you determine whether or not a particular network resource is responding on a network. Examples of network resources include desktop & laptop computers, printers, Xbox & Playstation 3 game systems, Cisco IP phones, Tandberg video conference units, projectors, websites of course, and even some household home appliances. By using the Ping command utility you can easily confirm that your computer can communicate with other network resources. If pinging a resource is unsuccessful this could be an indication of cable or network card issues, problems with a hub, switch, router, etc.On top of this the Ping command tool is a great way to verify that you can correctly communicate with a resource via its DNS name. If you cannot ping something by its DNS name but you can by its IP address, this could indicate a problem with DNS on a server, router, local workstation, etc.

## 7.2 Using the Ping Command

If you are having connectivity problems, you can use the **ping** command to check the destination IP address you want to reach and record the results. The **ping** command displays whether the destination responded and how long it took to receive a reply. If there is an error in the delivery to the destination, the **ping** command displays an **error message**.

You can use the **ping** command to:

- Ping your computer (by address, not **host name**) to determine that TCP/IP is functioning. (Pinging your computer does not verify that your network adapter is functioning.)
- Ping the local router to determine whether the router is running.
- Ping beyond your local router.

The following table shows some useful **ping** command options.

| Option | Use |
|---|---|
| **-n** *Count* | Determines the number of echo requests to send. The default is 4 requests. |
| **-w** *Timeout* | Enables you to adjust the time-out (in milliseconds). The default is 1,000 (a 1-second time-out). |
| **-l** *Size* | Enables you to adjust the size of the ping packet. The default size is 32 bytes. |
| **-f** | Sets the Do Not Fragment bit on the ping packet. By default, the ping packet allows fragmentation. |

**Table 7.1 Ping Command Options**

The following example illustrates how to send two pings, each 1,450 bytes in size, to IP address 131.107.8.1:

```
C:\>ping -n 2 -l 1450 131.107.8.1
Pinging 131.107.8.1 with 1450 bytes of data:

Reply from 131.107.8.1: bytes=1450 time<10ms TTL=32
Reply from 131.107.8.1: bytes=1450 time<10ms TTL=32

Ping statistics for 131.107.8.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate roundtrip times in milliseconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms
```

By default, **ping** waits 4,000 milliseconds (4 seconds) for each response to be returned before displaying the "Request Timed Out" message. If the remote system being pinged is across a high-delay link, such as a satellite link, responses may take longer to be returned. You can use the **-w** (wait) option to specify a longer time-out.

To check connectivity by using the **ping** command, at the command prompt, type **ping** and the IP address you want to reach.

A response of "Destination net unreachable" means there was no route to the destination. You need to check the **routing** table on the router listed in the "Reply from" address in the "Destination net unreachable" message. For more information about the routing table, see Understanding the IP routing table.

A response of "Request timed out" means that there was no response to the ping in the default time period (1 second). You can check for the following:

- A router is down.

To check the routers in the path between the source and the destination, use the **tracert** command. For more information, see Using the tracert command.

- The destination host is down.

  Physically verify that the host is running or check connectivity through another protocol.

- There is no route back to your computer.

  If the host is running, you can check for a return route by viewing the default gateway and local routing table on the destination host.

- The latency of the response is more than one second.

  Use the **-w** option on the **ping** command to increase the time-out. For example, to allow responses within 5 seconds, use **ping -w 5000**.

### 7. 3 Ipconfig

This command is most useful on computers that are configured to obtain an IP address automatically. This enables users to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration. If the Adapter name contains any spaces, use quotation marks around the adapter name (that is, "Adapter Name"). For adapter names, **ipconfig** supports the use of the asterisk (*) wildcard character to specify either adapters with names that begin with a specified string or adapters with names that contain a specified string.

For example, **Local*** matches all adapters that start with the string Local and ***Con*** matches all adapters that contain the string Con.This command is available only if the **Internet Protocol (TCP/IP)** protocol is installed as a component in the properties of a network adapter in Network Connections .Displays all current TCP/IP network configuration values and refreshes **Dynamic Host** Configuration Protocol (DHCP) and **Domain Name System** (DNS) settings. Used without parameters, **ipconfig** displays the IP address, subnet mask, and default gateway for all adapters.

**Syntax**

**ipconfig** [**/all**] [**/renew** [*Adapter*]] [**/release** [*Adapter*]] [**/flushdns**] [**/displaydns**] [**/registerdns**] [**/showclassid** *Adapter*] [**/setclassid** *Adapter* [*ClassID*]]

### 7.4 Parameters of Ipconfig

**/all :** Displays the full TCP/IP configuration for all adapters. Without this parameter, **ipconfig** displays only the IP address, subnet mask, and default gateway values for each adapter. Adapters can represent physical interfaces, such as installed network adapters, or logical interfaces, such as dial-up connections.

**/renew [ *Adapter* ] :** Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the *Adapter* parameter is included. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.

**/release [ *Adapter* ] :** Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the *Adapter* parameter is included. This parameter disables TCP/IP for adapters configured to obtain an IP address automatically. To specify an adapter name, type the adapter name that appears when you use **ipconfig** without parameters.

**/flushdns :** Flushes and resets the contents of the DNS client resolver cache. During DNS troubleshooting, you can use this procedure to discard negative cache entries from the cache, as well as any other entries that have been added dynamically.

**/displaydns :** Displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local Hosts file and any recently obtained resource records for name queries resolved by the computer. The DNS Client service uses this information to resolve frequently queried names quickly, before querying its configured DNS servers.

**/registerdns :** Initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer. You can use this parameter to troubleshoot a **failed** DNS name registration or resolve a dynamic update problem between a client and the DNS server without rebooting the client computer. The DNS settings in the advanced properties of the TCP/IP protocol determine which names are registered in DNS.

**/showclassid *Adapter* :** Displays the DHCP class ID for a specified adapter. To see the DHCP class ID for all adapters, use the asterisk (*****) wildcard character in place of *Adapter*. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically.

**/setclassid *Adapter* [ *ClassID* ] :** Configures the DHCP class ID for a specified adapter. To set the DHCP class ID for all adapters, use the asterisk (*****) wildcard character in place of *Adapter*. This parameter is available only on computers with adapters that are configured to obtain an IP address automatically. If a DHCP class ID is not specified, the current class ID is removed.

# 8. Develop a Program to Compute the Hamming Distance Between any Two Code Words.

**8.1 Data Bits or Word:** The actual data that is needed to be transmitted are called data bits or word.

**8.2 Control Bits:** The redundant information which is added with data bits so as to detect the error in data bits is called control bits.

**8.3 Coding:** The process of adding control bits to data bits is called coding.

**8.4 Code Words(c):** The data bits and control bits together are called codewords.

**8.5 Code Set:**The set of various valid code words is called codeset

**8.6 Hamming Distance(d):** In information theory, the **Hamming Distance** between two codewords of equal length is the number of positions at which the corresponding symbols are different. In another way, it measures the minimum number of substitutions required to change one string into the other, or the minimum number of errors that could have transformed one string into the other. In simpler words it is the number of positions at which two code words differ from each other.

Mathematically: **$d=c_1$ xor $c_2$**, where $c_1$ and $c_2$ are two different code words of equal lengths

For example: The Hamming distance between:

- "**karolin**" and "**kathrin**" is **3.**
- "**karolin**" and "**kerstin" is 3**.
- **1011101** and **1001001** is 2.
- **2173896** and **2233796** is 3.

In order to make a program for calculating the hamming distance between two code words following steps should be considered using any programming language.

1. Take two variables to store the two code word as input from the user such as ‘a’ and ‘b’.
2. Take a third variable ‘d’ to store the result of hamming distance calculation of two code words stored in variables ‘a’ and ‘b’ respectively.
3. Perform the xor operation on two code words using the operation ‘a’ xor ‘b’.
4. Store the result of step 3 in the variable d.
5. Print the resultant output stored in variable ‘d’ to the user**.**

# 9. Develop a Program to Compute Checksum for a _m'bit Frame using a Generator Polynomial.

Also called CRC (**Cyclic Redundancy Check**)
Data is sent with a checksum.
When arrives, **checksum** is recalculated. Should match the one that was sent.

Bitstring represents polynomial.
e.g. 110001 represents:
$1 . x^5 + 1 . x^4 + 0 . x^3 + 0 . x^2 + 0 . x^1 + 1 . x^0$
$= x^5 + x^4 + x^0$

The **order** of a polynomial is the power of the highest non-zero coefficient. This is polynomial of order 5.

**Modulo 2 arithmetic**

We are going to define a particular field (or here), in fact the smallest field there is, with only 2 members.

We define addition and subtraction as modulo 2 with no carries or borrows. This means addition = subtraction = XOR. Here's the rules for addition:

```
0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0
```

Multiplication:

```
0 * 0 = 0
0 * 1 = 0
1 * 0 = 0
1 * 1 = 1
```

Subtraction: if 1+1=0, then 0-1=1, hence:

```
0 - 0 = 0
0 - 1 = 1
1 - 0 = 1
1 - 1 = 0
```

Long division is as normal, except the subtraction is modulo 2.

## Example

No carry or borrow:

```
011 + (or minus)
110
---
```

`101`
Consider the polynomials:
$x + 1 +$
$x^2 + x$
---
$x^2 + 2x + 1$
$= x^2 + 1$
We're saying the polynomial arithmetic is modulo 2 as well, so that:
$2\ x^k = 0$ for all k.

The General CRC Generator block generates cyclic redundancy code (CRC) bits for each input data frame and appends them to the frame. This block accepts a binary column vector input signal.

You specify the generator polynomial for the CRC algorithm using the **Generator polynomial** parameter. This block is general in the sense that the degree of the polynomial does not need to be a power of two. You represent the polynomial in one of these ways:

- As a binary row vector containing the coefficients in descending order of powers. For example, `[1 1 0 1]` represents the polynomial $x^3 + x^2 + 1$.
- As an integer row vector containing the powers of nonzero terms in the polynomial, in descending order. For example, `[3 2 0]` represents the polynomial $x^3 + x^2 + 1$.

You specify the initial state of the internal shift register by the **Initial states** parameter. The **Initial states** parameter is either a scalar or a binary row vector of length equal to the degree of the generator polynomial. A scalar value is expanded to a row vector of length equal to the degree of the generator polynomial. For example, the default initial state of `[0]` is expanded to a row vector of all zeros.

You specify the number of checksums that the block calculates for each input frame by the **Checksums per frame** parameter. The **Checksums per frame** value must evenly divide the size of the input frame. If the value of **Checksums per frame** is *k*, the block does the following:

1. Divides each input frame into *k* subframes of equal size
2. Prefixes the **Initial states** vector to each of the *k* subframes
3. Applies the CRC algorithm to each augmented subframe
4. Appends the resulting checksums at the end of each subframe
5. Outputs concatenated subframes

If the size of the input frame is *m* and the degree of the generator polynomial is *r*, the output frame has size $m + k * r$.