connection. User data is interspersed in-band with Telnet control information in an 8-bitbyte oriented data connection over the **T**ransmission **C**ontrol **P**rotocol (**TCP**).

Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration (including systems based on Windows NT). Because of security issues with Telnet, its use for this purpose has waned in favour of SSH.

6 HTTP

The **H**ypertext **T**ransfer **P**rotocol (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Hypertext is a multi-linear set of objects, building a network by using logical links (the so-called hyperlinks) between the nodes (e.g. text or words). HTTP is the protocol to exchange or transfer hypertext.

7 SSH File Transfer Protocol

In computing, the SSH **F**ile **T**ransfer **P**rotocol (also **S**ecure **F**ile **T**ransfer **P**rotocol, **S**ecure **FTP**, or **SFTP**) is a network protocol that provides file access, file transfer, and file management functionalities over any reliable data stream.

It was designed by the **I**nternet **E**ngineering **T**ask **F**orce (**IETF**) as an extension of the **S**ecure **S**hell **P**rotocol (**SSH**) version 2.0 to provide secure file transfer capability, but is also intended to be usable with other protocols.

The IETF of the Internet Draft states that even though this protocol is described in the context of the SSH-2 protocol, it could be used in a number of different applications, such as secure file transfer over **T**ransport **L**ayer **S**ecurity (**TLS**) and transfer of management information in VPN applications.

This protocol assumes that it is run over a secure channel, such as SSH, that the server has already authenticated the client, and that the identity of the client user is available to the protocol.

8 Post Office Protocol

In computing, the **P**ost **O**ffice **P**rotocol (**POP**) is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. POP and IMAP (Internet Message Access Protocol) are the two most prevalent Internet standard protocols for e-mail retrieval.

Virtually all modern e-mail clients and servers support both. The POP protocol has been developed through several versions, with version 3 (POP3) being the current standard. Most webmail service providers such as Hotmail, Gmail and Yahoo! Mail also provide IMAP and POP3 service.

Networking Components

- **Gateway:** A device sitting at a network node for interfacing with another network that uses different protocols. Works on OSI layers 4 to 7.
- **Router:** A specialized network device that determines the next network point to which it can forward a data packet towards the destination of the packet. Unlike a gateway, it cannot interface different protocols. Works on OSI layer 3.
- **Switch:** A device that allocates traffic from one network segment to certain lines (intended destination(s)) which connect the segment to another network segment. So unlike a hub a switch splits the network traffic and sends it to different destinations rather than to all systems on the network. Works on OSI layer 2.
- **Bridge:** A device that connects multiple network segments along the data link layer. Works on OSI layer 2.
- **Hub:** It connects multiple Ethernet segments together making them act as a single segment. When using a hub, every attached device shares the same broadcast domain and the same collision domain. Therefore, only one computer connected to the hub is able to transmit at a time.

  Depending on the network topology, the hub provides a basic level 1 OSI model connection among the network objects (workstations, servers, etc.). It provides bandwidth which is shared among all the objects, compared to switches, which provide a connection between individual nodes.
- **Repeater:** A device to amplify or regenerate digital signals received while sending them from one part of a network into another. Works on OSI layer 1.
- **Modem (MoDem):** A device that **mo**dulates an analog "carrier" signal (such as sound), to encode digital information, and that also **dem**odulates such a carrier signal to decode the transmitted information, as a computer communicating with another computer over the telephone network

Types of MODEM

External Modem: This is a modem separated from the system unit in the computer case. It is connected to the serial port of the computer by means of a cable. It is connected to the telephone wall jack by another cable.

Internal Modem: An internal modem is a circuit board (a modem card) that can be added to the system unit of the computer. It takes one of the expansion slots.

Wired Modem / Standard Modem

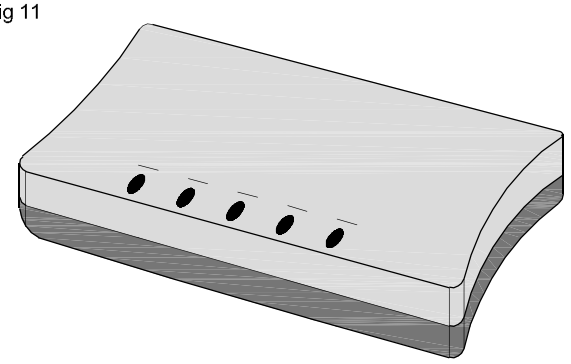
Most modem's used today are called standard modems. These modems are usually operated by commands entered from a microcomputer keyboard. Users control the functions (dialling, etc.) of a modem through the keyboard. Modems may use different command languages to control their functions,

Wireless Modems: Wireless modems transmit the data signals through the air instead of by using a cable. They sometimes are called a radiofrequency modem. This type of modem is designed to work with cellular technology, and wireless local area networks. Wireless modems are not yet perfected, but the technology is rapidly improving.

ADSL Modem

Asymmetric **D**igital **S**ubscriber **L**ine, ADSL (Fig 11) is a type of DSL broadband communications technology used for connecting to the Internet. ADSL allows more data to be sent over existing copper telephone lines POTS, when compared to traditional modem lines. A special filter, called a micro filter, is installed on a subscriber's telephone line to allow both ADSL and regular voice (telephone) services to be used at the same time. ADSL requires a special ADSL modem and subscribers must be in close geographical locations to the provider's central office to receive ADSL service. Typically this distance is within a radius of 2 to 2.5 miles. ADSL supports data rates of from 1.5 to 9 Mbps when receiving data (known as the down-stream rate) and from 16 to 640 Kbps when sending data (known as the up- stream rate).

Fig 11



DNA - A211 - I ADSL2 + MODEM

CP150118

Network Interface Card (NIC)

NIC (Fig. 12) provides the hardware interface between a computer and a network. A NIC technically is network adapter hardware in the form factor of an add-in card such as a PCI or PCMCIA card. Some NIC cards work with wired connections while others are wireless. Most NICs support either wired Ethernet or WI-FI wireless standards.

12

Ethernet NICs plug into the system bus of the PC and include jacks for network cables, while WI-FI NICs contain built-in transmitters / receivers (transceivers). In new computers, many NICs are now pre-installed by the manufacturer. All NICs feature a speed rating such as 11 Mbps, 54 Mbps or 100 Mbps that suggest the general performance of the unit.

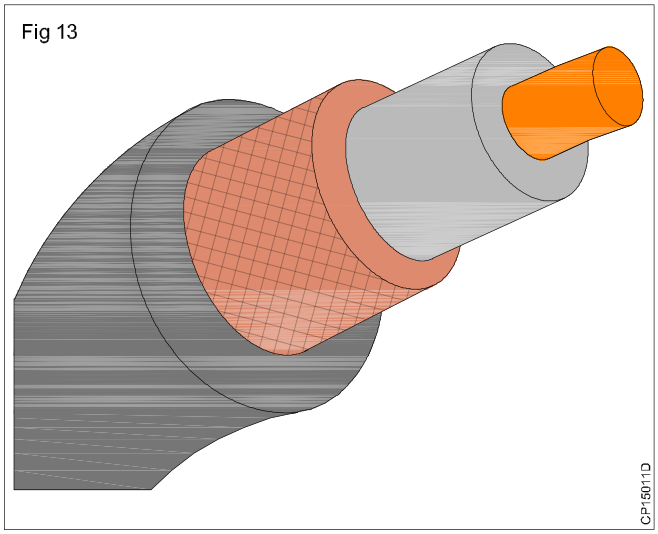
Network Cables Standards

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.

Cable standards

A wide range of cabling types are been used to run Ethernet systems. Therefore, different types of cabling standards are being used for the networks involved in connecting devices together using different types of cabling system.

Fig 13



CP150117D

Coaxial cable (Fig 13) is the kind of copper cable used by companies between the community antenna and user homes and businesses. Coaxial cable is sometimes used by telephone companies from their central office to the telephone poles near users. It is also widely installed for use in business and corporation and other types of.

Coaxial cable is called "coaxial" because it includes one physical that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.

10BASE-T Cable Standard: 10Base-T is one of the Ethernet standards for cabling in a network environment. 10BaseT uses a twisted pair cable with a maximum length

of 100 meters. Standard 10BaseT operates at 10 Mbps. It is commonly used in a star topology.

10BASE-FL Cable Standard: 10BaseFL is a fibber optic cable standard designed to run at 10 Mbps. It is similar to 10Base-T, though the media type is fibber. For use up to 2000 meters.

100BASE-TX Cable Standard: 100 Mbps Fast Ethernet over category 5 twisted pair cable. Maximum cable length of 100 meters.

100BASE-FX Cable Standard: 100 Mbps Fast Ethernet standard over fibber cable. Can transmit data up to 2000 meters.

1000BASE-T Cable Standard: Gigabit Ethernet over twisted pair copper wires. Transmit up to 1000 Mbps. 100 meter maximum cable length. Cat5 or better required (Cat6 cabling recommended).

1000BASE-CX Cable Standard: Gigabit Ethernet over a special copper twinax cable. Up to 25 meters in length. Typically used in a wiring closet or data center as a short jumper cable.

1000BASE-SX Cable Standard: Gigabit Ethernet using a short-wavelength laser device over multimode fibber optic cable. 50 µm core (max 300 meters) or 62.5 µm core (max 500 meters). 1000Mbps maximum transfer speed.

1000BASE-LX Cable Standard: Gigabit Ethernet using long-wavelength laser transmitters over fibber optic cable. Up to 3,000 meters. Uses single mode fibber and requires SC connectors for terminating the cable.

10 GBASE-SR Cable Standard: 802.3ae standard. 33 meters for 62.5µm fibber optic cable, 300 meters for 50µm cables. 10 Gbps (Gigabit per second) transfer rate.

10 GBASE-LR Standard: 10 Gbps transfer rate. 10 kilometres maximum distance. Fibber optic cable.

10 GBASE-ER Standard: 10 Gbps transfer rate. 40 kilometres maximum cable length. Fibber optic cable.

Media types

A cable is a device which contains a number of signal conductors usually in the form of separate wires. It is the medium through which information usually moves from one system to another through the network. There are several types of cable which are commonly used with the local area network. In some cases, a network utilizes only one types of cable, whereas other network uses a variety of cable types. The type of cable chosen for a network is related to network topology, protocol and size.

Twisted Pair

Twisted pair cable is the most common type of network medium used in LAN today. A transmission media consist of colour coded pairs of two shielded insulated copper wires which are arranged in a spiral pattern. The spiral pattern is an important aspect of twisted - pair cables in order to minimize cross talk of interference between adjoining wires.

The advantage of using twisted pair cables are

- It is lighter, thinner and more flexible
- Easy to install
- It is in expensive

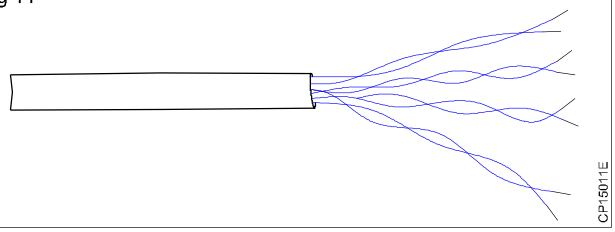
There are two varieties of twisted pair cabling, they are

- **U**nshielded **T**wisted **P**air (**UTP**)
- **S**hielded **T**wisted **P**air (**STP**)

Unshielded twisted pair (UTP)

Unshielded twisted pair (Fig 14) cabling consists of two unshielded wires twisted around each other that contain no shielding. It is commonly used in the telephone wires and is common for computer networking because of high flexibility of the cables. It is a plastic connector that looks like a large telephone-style connector. The standard connector for unshielded twisted pair cabling is RJ-45 connector.

Fig 14



UTP has five categories of cable standards defined by the Electronic Industries Association and Telecommunications Industry Association (commonly known as EIA/TIA). The five categories of unshielded twisted pair are:

Categories of Unshielded Twisted Pair

In order to manage the network cabling, you need to be familiar with the standards that may be used on modern networks. The categories of the unshielded twisted pair cable are described below.

Category 1

- It is a form of UTP that contains two pairs of wire.
- CAT is suitable for voice communications but not for data.
- It can carry up to 128 kilobits per second (Kbps) of data.
- It is usually used for telephone wire Data rate - 1 Mbps. This type of wire is not capable of supporting computer network traffic and is not twisted.

Category 2

- It contains four wire pairs and can carry up to 4 Mbps of data.
- CAT 2 is rarely found on modern networks.
- Category 2 or CAT 2 is capable of transmitting data up to 4 Mbps. This of cable is seldom used.

Category 3

- CAT 3 made up of four twisted - pair wires, each twist is three times per foot. It is certified to transmit data up to 10 Mbps.
- CAT 3 has typically been used for 10 Mbps Ethernet or 4 Mbps Token Ring networks.
- The CAT 3 cabling is gradually replaced with CAT5 to accommodate higher throughput.

Category 4

- CAT 4 is made up of four twisted-pair wires, specialized to transmit data up to 16 Mbps and is rarely is used in new installations.
- CAT 4 may be used for 16Mbps Token Ring or 10 Mbps Ethernet networks. It is guaranteed for signals as high as 20 MHz and Provides More protection against crosstalk and attenuation than CAT1, CAT2, orCAT 3.

Category 5

- CAT 5 is the most popular twisted pair Ethernet cabling designed for high signal integrity which is in common use today.
- CAT 5 contains four wire pairs and supports up to 100 Mbps throughout.
- It is the most popular form of UTP for new network installations and upgrades to Fast Ethernet.
- In addition to 100 Mbps Ethernet, CAT 5 wiring can support other fast networking technologies.
- It is popular because it is both affordable and high speed for today's local area networks Cat 5 cables are often used in structured cabling for computer networks such as fast Ethernet.

Category 6

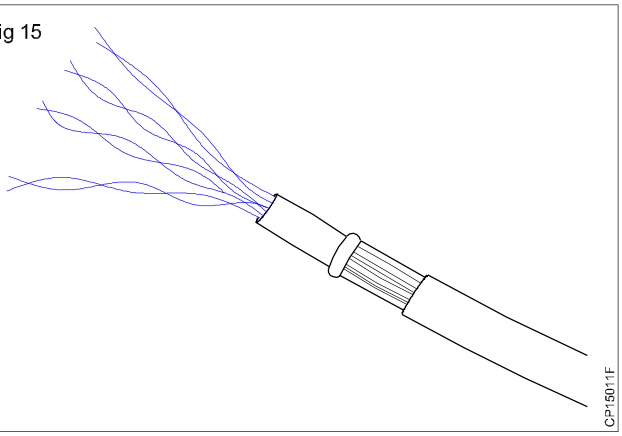
- CAT 6 cable was originally designed to support gigabit Ethernet. It is similar to CAT 5 wire, but contains a physical separator between the four

  Twisted copper wires pairs to further reduce the electromagnetic interference.
- It is a twisted-pair cable that contains four wire pairs, each wrapped in foil insulation. Additional foil insulation covers the bundle of wire pairs, and a fire-resistant plastic sheet covers the second foil layer.
- The foil insulation provides excellent resistance to crosstalk and enables CAT 6 to support at least six times the throughput supported by regular CAT 5.
- When the CAT 6 is used as a patch cable, it is usually terminated in RJ-45 Electrical connectors.

Shield Twisted Pair (Fig 15)

A type of copper telephone wiring in which each of the two copper wires that are twisted together are coated with an insulating coating that functions as a ground for the wires.

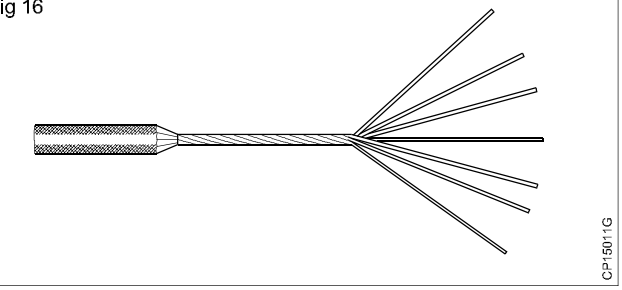
Fig 15



The extra covering in shielded twisted pair wiring protects the transmission line from leaking into or out of the cable. STP cabling often is used in networks, especially fast data rate Ethernets.

Fiber Optic Cable (Fig 16)

Fig 16



A technology that uses glass (or plastic) threads (fibers) to transmit. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages on to light waves.

Fibre optics has several advantages over traditional metal lines:

- Fibre optic cables have a much greater than metal cables. This means that they can carry more data.
- Fibre optic cables are less susceptible than metal cables to interference.
- Fibre optic cables are much thinner and lighter than metal wires.
- Data can be transmitted (the natural form for data) rather than analogically.

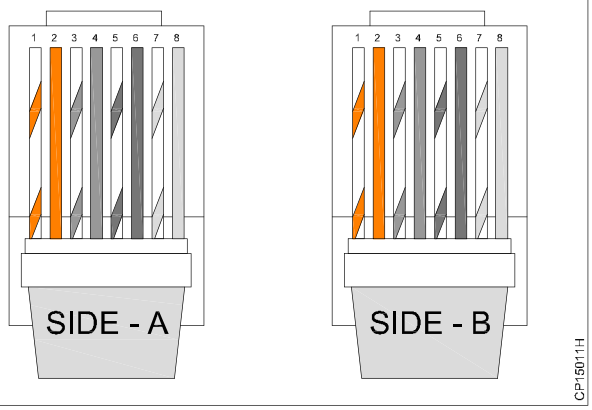
The main disadvantage of fibre optics is that the cables are expensive to install. In addition, they are more fragile than wire and are difficult to splice.

In addition, telephone companies are steadily replacing traditional telephone lines with fibre optic cables. In the future, almost all communications will employ fibre optics.

Straight Cable

A straight cable (Fig 17) is to connect different type of devices. This type of cable will be used most of the time and can be used to:

Fig 17



1 Connect a computer to a switch/hub's normal port.

2 Connect a computer to a cable/DSL modem's LAN port.

3 Connect a router's WAN port to a cable/DSL modem's LAN port.

4 Connect a router's LAN port to a switch/hub's uplink port. (Normally used for expanding network)

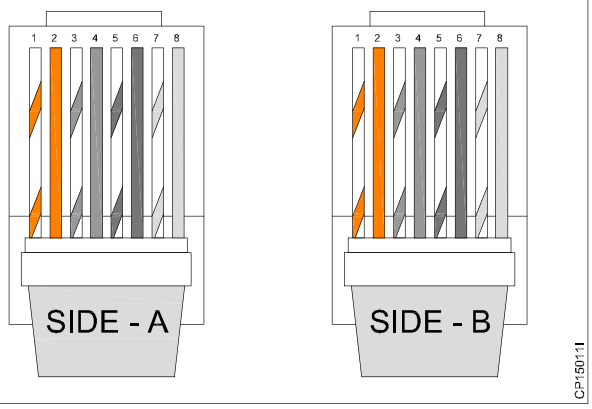
5 Connect 2 switches/hubs with one of the switch/hub using an uplink port and the other one using normal port.

If you need to check how straight cable looks like, it's easy. Both sides (side A and side B) of cable have wire arrangement with same colour.

Crossover Cable

A crossover cable (Fig 18), it's usually used to connect same type of devices. A crossover cable can be used to:

Fig 18



1 Connect 2 computers directly.

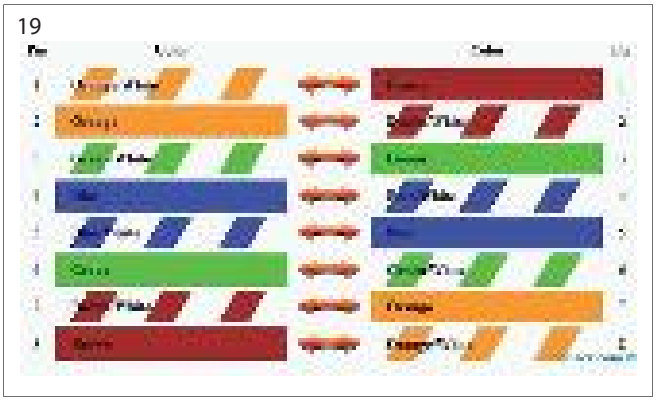
2 Connect a router's LAN port to a switch/hub's normal port. (Normally used for expanding network).

3 Connect 2 switches/hubs by using normal port in both switches/hubs.

In you need to check how crossover cable looks like, both side (side A and side B) of cable have wire arrangement with following different colour.

Rollover Cable (Fig 19)

19



Rollover cable (also known as **Cisco Console Cable** or a **Yost Cable**) is a type of cable that is often used to connect a computer terminal to a router's port. This cable is typically flat (and has a light blue colour) to help distinguish it from other types of network cabling. It gets the name rollover because the pin outs on one end are reversed from the other, as if the wire had been rolled over and you were viewing it from the other side.

Connectors

The media connectors are the physical devices that help to transfer the data between the systems.

RJ11: Registered **J**ack-**11** (Fig 20) a four- or six-wire used primarily to connect telephone equipment. RJ-11 connectors are also used to connect some types of some types of Local area network.

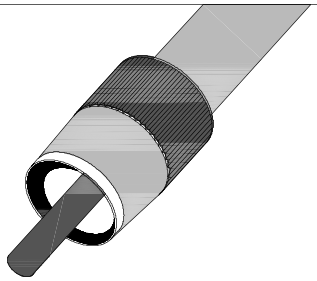
20

RJ45: RJ45 (Fig 21) connectors feature eight pins to which the wire strands of a cable interface electrically. Standard RJ-45 pinouts define the arrangement of the individual wires needed when attaching connectors to a cable.

ST: ST stands for **S**traight **T**ip (Fig 22) - a quick release bayonet style developed by AT&T. STs were predominant in the late 80s and early 90s.

21

Fig 22



CP15011M

ST Connectors are among the most commonly used fiber optic connectors in networking applications. They are cylindrical with twist lock coupling, 2.5mm keyed ferrule. ST connectors are used both short distance applications and long line systems.

SC: SC stands for **S**ubscriber **C**onnector (Fig 23) - a general purpose push/pull style Connector developed by NTT. SC has an advantage in keyed duplexibility to support send/receive channels.

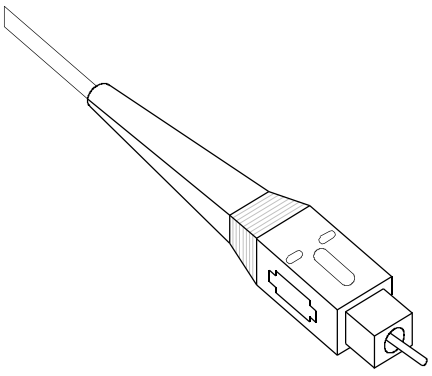
SC Connectors are frequently used for newer Network applications. The SC is a snap-in connector that is widely used in single mode systems for its performance. The SC connector is also available in a Duplex configuration. They offer low cost, simplicity, and durability. SC connectors provide for accurate alignment via their ceramic ferrules.

The square, snap-in connector latches with a simple push-pull motion and is keyed. They feature a 2.5mm Ferrule and molded housing for protection. Typical matched SC connectors are rated for 1000 mating cycles and have an Insertion Loss of 0.25 dB.

LC: LC stands for **L**ucent **C**onnector (Fig 24). The LC is a small form factor fiber optic connector.

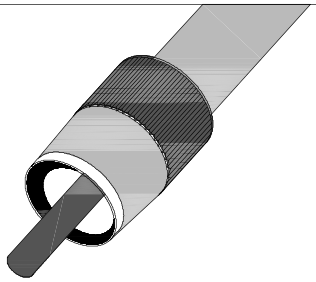
The LC Connector uses a 1.25 mm ferrule, half the size of the ST. Otherwise, it is a standard ceramic Ferrule connector. The LC has good performance and is highly favoured for single mode.

Fig 23



CP15011N

Fig 22



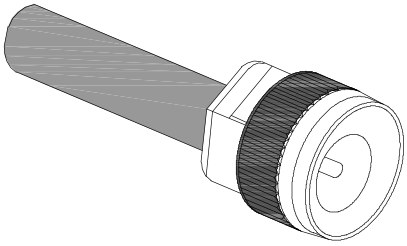
CP15011M

USB: The USB 2.0 Standard-A type of USB plug is a flattened rectangle which inserts into a "downstream-port" receptacle on the USB host, or a hub, and carries both power and data. This plug is frequently seen on cables that are permanently attached to a device, such as one connecting a keyboard or mouse to the computer via USB connection.

A Standard-B plug-which has a square shape with bevelled exterior corners-typically plugs into an "upstream receptacle" on a device that uses a removable cable, e.g. a printer. A Type B plug delivers power in addition to carrying data. On some devices, the Type B receptacle has no data connections, being used solely for accepting power from the upstream device. This two-connector-type scheme (A/B) prevents a user from accidentally creating an Electrical loop.

BNC: Bayonet **N**eill **C**oncelman (Fig 25) connector, (sometimes erroneously called a British Naval Connector or Bayonet Nut Connector, a type of connector used with coaxial cable such as the RG-58 A/U cable used with the 10Base2. The basic BNC connector is a male type mounted at each end of a cable.

Fig 25



CP15011P

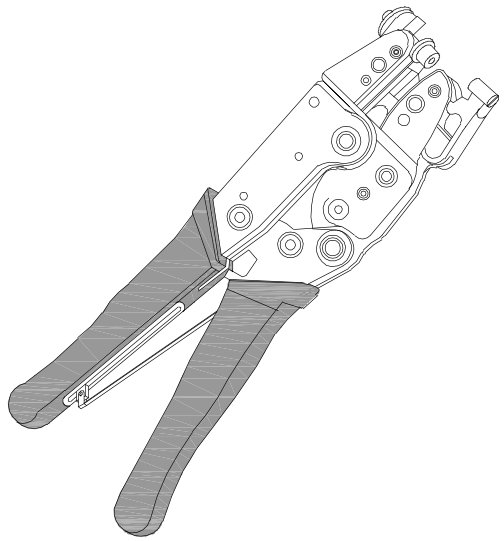
This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector.

BNC T-connectors (used with the 10Base-2 system) are female devices for connecting two cables to a NIC. A BNC barrel connector allows connecting two cables together.

BNC connectors can also be used to connect some monitor, which increases the accuracy of the signals sent from the adapter.

Crimping Tool: A crimping tool (Fig 26) 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 RJ45 and RJ11 connectors to the end of the cable. In the picture to the right, is an example of what a crimping tool looks like. This shows a tool capable of crimping both RJ-11 and RJ-45 connectors.

Fig 26



How to Crimp RJ45

1 Strip 1 to 2 inches (2.5 to 5.1 cm) of the outer skin at the end of the cable wire by making a shallow cut in the skin with a utility knife. Run the knife around the cable, and the jacket should slide off easily. There will be 4 pairs of twisted wires exposed, each of them a different color or colour combination.

   Orange-white striped and solid orange

   Green-white striped and solid green

   Blue-white striped and solid blue

   Brown-white striped and solid brown

2 Fold each pair of wires backwards to expose the core of the cable.

3 Cut off the core and discard.

4 Straighten the twisted wires using 2 pair of tweezers. Grasp a wire beneath a bend with 1 pair of tweezers, and use the other pair to gently straighten the bend. The straighter your wires, the easier your job will be

5 Arrange the untwisted wires in a row, placing them into the position, running from right to left, in which they will go into the RJ-45 connector:

   - Orange with a white stripe
   - Orange
   - Green with a white stripe
   - Blue
   - Blue with a white strip
   - Green
   - Brown with a white stripe
   - Brown

6 Trim the untwisted wires to a suitable length by holding the RJ-45 connector next to the wires. The insulation on the cable should be just inside the bottom of the RJ-45 connector. The wires should be trimmed so that they line up evenly with the top of the RJ-45 connector.

   - Trim the wires in small increments, checking frequently to ensure a correct fit. It's better to cut the untwisted wires a few times than have to go back and start all over again because you trimmed off too much.

7 Insert the wires into the RJ-45 connector, making sure that they stay aligned and each color goes into its appropriate channel. Make sure that each wire goes all the way to the top of the RJ-45 connector. If you don't make these checks, you will find that your newly crimped RJ-45 connector is useless.

8 Use the crimping tool to crimp the RJ-45 connector to the cable by pressing the jacket and cable into the connector so that the wedge at the bottom of the connector is pressed into the jacket.

Re crimp the cable once more to ensure proper connection.

9 Follow the instructions above to crimp an RJ-45 connector to the opposite end of the cable

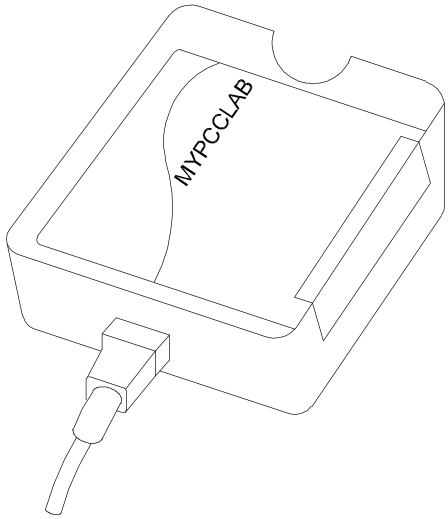
10 Use a cable tester to assure that your cable is working properly when both ends are crimped.

Cable Tester (Fig 27)

When connected to an Ethernet cable, a network cable tester tells if the cable is capable of carrying an Ethernet signal. If the cable carries the signal, this indicates that all the circuits are closed, meaning that electric current can move unimpeded through the wires, and that there are no short circuits, or unwanted connections, in the wire.

Network cable testers vary in complexity and price, but a basic tester consists of a source of electrical current, a measuring device that shows if the cable is good, and a connection between the two, usually the cable itself.

Fig 27



Computer networks use Ethernet cables to allow computers in the network to "talk" to each other. An Ethernet cable has eight wires that are arranged in four pairs. For current to flow correctly, the wire pairs must be connected in the proper order.

A network cable tester can identify if the wires are paired correctly. It can also show if there is a break in the insulation, a situation which allows crosstalk between two wires that should not be connected. The tester can also tell whether the cable has the proper level of resistance.

A network cable tester can be a simple apparatus that merely identifies whether current flows through the cable, or it may be a professional-level, complex device that gives additional information that helps identify the problem.

Professional-level network cable testers may not only tell if an open circuit exists, but may identify where the break is located. Some also identify the gauge of wire used and can generate their own signal to test for interference.

How to Check with the Tester

1 Turn on your network cable tester.

2 Plug one end of the Ethernet cable you are trying to test into the "IN" Ethernet input on the network cable tester.

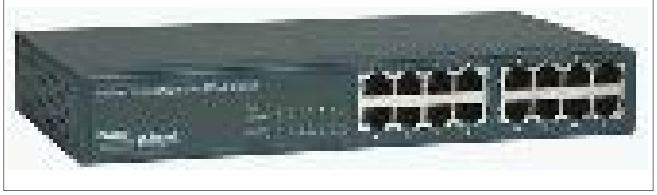
3 Plug the other end of your Ethernet cable you are trying to test into the "OUT" input on the network cable tester.

4 Press the "Test" button. The network cable tester will send a signal across the Ethernet cable. If the signal gets from one end of the cable to the other, a green light will appear on the device, letting you know that the test was successful. If the signal does not get from one end of the cable to the other, a red light will appear on the device, letting you know that the test was not successful and that the cable is bad.

Switch

A **Network Switch** (Fig 28) is a small hardware device that joins multiple computers together within one Local Area Network. Technically, network switches operate at layer two (Data Link Layer) of the OSI.

28



Network switches appear nearly identical to hub, but a switch generally contains more intelligence (and a slightly higher price tag) than a hub. Unlike hubs, network switches are capable of inspecting data packet as they are received, determining the source and destination device of each packet, and forwarding them appropriately.

By delivering messages only to the connected device intended, a network switch conserves bandwidth and offers generally better performance than a hub.

Availability of Switches

1 8 Port Switches

2 16 port switches

3 24 port switches

4 32 port switches

Hub: A Hub (Fig 29) is a small, simple, inexpensive device that joins multiple computers together. Many network hubs available today support the Ethernet standard. Other types including USB hubs also exist, but Ethernet is the type traditionally used in home networking.

To network a group of computers using an Ethernet hub,

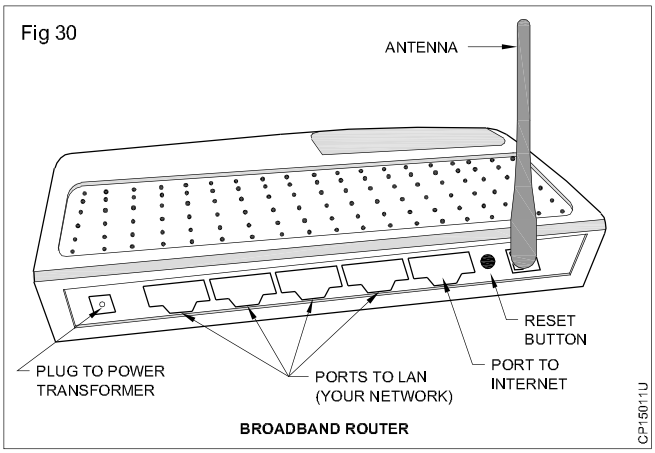
29

first connect an Ethernet cable into the unit, and then connect the other end of the cable to each computer's NIC. All Ethernet hubs accept the RJ45 connectors of standard Ethernet cables.

Ethernet hubs vary in the speed (network data rate or bandwidth they support. Some years ago, Ethernet hubs offered only 10 Kbps rated speeds. Newer types of hubs offer 100 Mbps Ethernet. Some support both 10 Mbps and 100 Mbps (so-called dual-speed or 10/100 hubs).

Routers

Routers (Fig 30) are physical devices that join multiple wired or wireless networks together. Technically, a wired or wireless router is a Layer 3 gateway, meaning that the wired/wireless router connects networks (as gateways do), and that the router operates at the network layer of the OSI model.



Home networkers often use an Internet Protocol (IP) wired or wireless router, IP being the most common OSI network layer protocol. An IP router such as a DSL or cable modem router joins the home's LAN to the WAN of the Internet.

Bridges

A bridge (Fig 31) device filters data traffic at a network boundary. Bridges reduce the amount of traffic on a 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.

ISP: Internet **S**ervice **P**rovider, it refers to a company that provides Internet services, including personal and business access to the internet. For a monthly fee, the service provider usually provides a software package, Username, password and access phone number.

Equipped with a modem you can then log on to the Internet and browse the world wide web and USENET and send and receive email For broadband access you typically receive the broadband modem hardware or pay a monthly fee for this equipment that is added to your ISP account billing.

In addition to serving individuals, ISPs also serve large companies, providing a direct connection from the company's networks to the Internet. ISPs themselves are connected to one another through Network Access Point (NAPs). ISPs may also be called IAPs (Internet Access Provider).

State Owned ISP's

- **BSNL** - Servicing all of India except Mumbai and Delhi. Triple-play Broadband Services provided by ADSL and VDSL. Also providing internet services over GPRS, 3G, as well as WiMax
- **MTNL** - Servicing Mumbai and Delhi. Triple-play Broadband Services provided by ADSL under the "Tri-Band" brand. Also providing GPRS and 3G internet services.

Private Owned nationwide ISP's

- Airtel - ADSL, GPRS, 3G & 4G LTE
- Skynet Broadband - Internet Service Provider
- Aircel - GPRS & 3G
- Hathway - Broadband over Cable
- Idea - GPRS & 3G
- MTS India - CDMA/EV-DO
- O-Zone Networks Private Limited - Pan - India Public Wi-Fi hotspot provider
- Reliance Communications - ADSL, GPRS & 3G, Metro-Ethernet, CDMA/EV-DO, Wimax
- Reliance Industries - LTE (to be launched)
- Sify - Broadband over cable
- Tata DoCoMo - GPRS & 3G
- Tata Indicom - ADSL, CDMA/EV-DO, Metro-Ethernet, WiMax
- Vodafone - GPRS & 3G

NSP: Network **S**ervice **P**roviders (**NSP**) is a business or organization that sells bandwidth or network access by providing direct Internet backbone access to the Internet and usually access to its **N**etwork **A**ccess **P**oint (**NAP**s).

Network service providers may consist of Telecommunications companies, data carriers, wireless communications providers, Internet service provider, and Cable television operators offering high-speed Internet access.

Dial up: Dial-up access is really just like a phone connection, except that the parties at the two ends are computer devices rather than people. Because dial-up access uses normal telephone lines, the quality of the connection is not always good and data rate are limited.

In the past, the maximum data rate with dial-up access was 56 Kbps (56,000 bits per second), but new technologies such as ISDN are providing faster rates.

Broadband: The term broadband refers to a telecommunications signal or device of greater Bandwidth (signal processing), in some sense, than another standard or usual signal or device (and the broader the band, the greater the capacity for traffic).

Wireless (Wi-Fi): Wireless broadband is high-speed Internet service via wireless technology. Wireless broadband is available in Internet cafés, local "hot spots" within many cities, private businesses and many homes.

The advantage of wireless broadband is that the computer receiving the Internet signal need not be tethered by an Ethernet or network cable to the broadband modem or router.

A wireless broadband modem receives the service and transmits it via radio waves to the immediate surrounding area. Any computer equipped with wireless capacity within receiving distance can pick up the signal, making the Internet 'portable.' The most common way to take advantage of wireless broadband is by using a laptop computer.

Mobile Broadband: The term mobile broadband refers to high-speed wireless Internet connections and services designed to be used from arbitrary locations.

Cellular networks normally provide broadband connections suitable for mobile access. The technologies in use today fall into two categories -3G (third generation cell networks) and 4G (fourth generation).

Introduction to TCP/IP

Objectives : At the end of this lesson you shall be able to
- **explain TCP/IP, addresses and subnets.**

Introduction to TCP/IP : TCP and IP were developed by Department of Defense (DOD) research project to connect a number different networks designed by different vendors into a network of networks (the "Internet"). It was initially usccessful because it delivered a few basic services that everyone needs (file transfer, electronic mail, remote logon) across a very large number of client and server systems. Several computers in a small department can use TCP/IP (along with other protocols) on a single LAN. The IP component provides routing from the department to the enterprise network, then to regional networks, and finally to the global internet. On the battlefield a communications network will sustain damage, so the DOD designed TCP/IP to be robust and automatically recover from any node or phone failure. This design allows the construction of very large networks with less central management. However, because of the automatic recovery, network problems can go undiagnosed and uncorrected for long periods of time.

As with all other communications protocol, TCP/IP is composed of layers:

IP is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination address (the IP number). The Internet authorities assign ranges of numbers to different organisations. The organisations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organisation to region and then around the world.

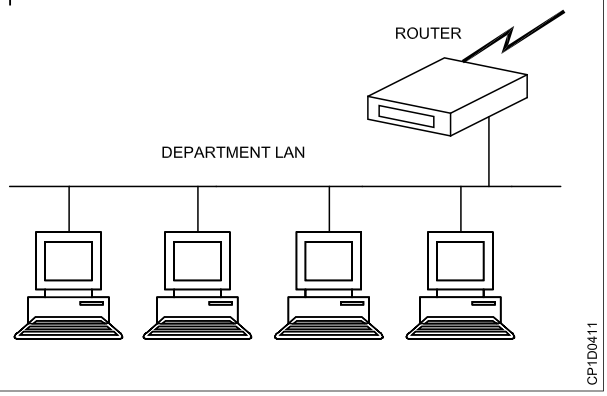
TCP is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.

Sockets is a name given to the package of subroutines that provide access to TCP/IP on most systems.

The Internet Protocol was developed to create a Network of Networks (the "Internet"). Individual machines are first connected to a LAN (Ethernet or Token Ring). TCP/IP shares the LAN with other users (a Novell file server, Windows for Workgroups peer systems). One device provides the TCP/IP connection between the LAN and the rest of the world. (Refer Fig 1)

To insure that all types of systems from all vendors can communicate, TCP/IP is absolutely standardised on the LAN. However, larger networks based on long distances and phone lines are more volatile. In US, many large corporations would wish to reuse large internal networks based on IBM's SNA. In Europe, the national phone

Fig 1



companies traditionally standardize on X.25. However, the sudden explosion of high speed microprocessors, fiber optics and digital phone systems has created a burst of new options: ISDN, frame relay, FDDI, Asynchronous Transfer Mode (ATM). New technologies arise and become obsolete within a few years. With cable TV and phone companies competing to built the National Information Superhighway, no single standard can govern citywide, nationwide, or worldwide communications.

The original design of TCP/IP as a Network of Networks fits nicely within the current technological uncertainty. TCP/IP data can be sent across a LAN or it can be carried within an internal corporate SNA network or it can piggyback on the cable TV service. Furthermore, machines connected to any of these networks can communicate to any other network through gateways supplied by the network vendor.

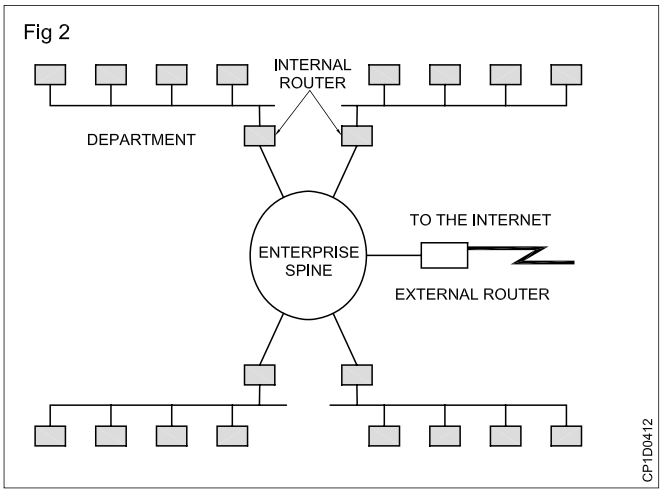
Addresses : Each technology has its own convention for transmission messages between two machines within the same network. On a LAN, messages are sent between machines by supplying the six byte unique identifier (the "MAC" address). In an SNA network, every mahine has Logical Units with their own network address. DECNET, Appletalk and Novell IPX all have a scheme for assigning numbers to each local network and to each workstation attached to the network.

On top of these local or vendor specific network addresses, TCP/IP assigns a unique number to every workstation in the world. This "IP number" is a four byte value that, by convention, is expressed by converting each byte into a decimal number (0 to 255) and separating the bytes with a period. For example, a server IP is like 130.132.59.234

Subnets: Although the individual subscribers do not need to tabulate network numbers or provide explicit routing, it is convenient for most Class B networks to be internally manage as much smaller and simpler version

of the larger network organisations. It is common to subdivide the two bytes available for internal assignment into a one byte department number and a one byte workstation ID. (Refer Fig 2)

Fig 2



The enterprise network is built using commercially available TCP/IP router boxes. Each router has small tables with 255 entries to translate the one byte department number into selection of a destination Ethernet connected to one of the routers.

TCP treats the data as a stream of bytes. It logically assigns a sequence number to each byte. The TCP packet has a header that says, in effect, “This packet starts with byte 379642 and contains 200 bytes of data.” The receiver can detect missing or incorrectly sequenced packets. TCP acknowledges data that has been received and retransmits data that has been lost. The TCP design means that error recovery is done end-to-end between the Client and Server machine. There is no formal standard for tracking problems in the middle of the network, though each network has adopted some adhoc tools.

There are three levels of TCP/IP knowledge. Those who administer a regional or national network must design a system of long distance phone lines, dedicated routing devices and very large configuration files. They must know the IP numbers and physical locations of thousands of subscriber networks. They must also have a formal network monitor strategy to detect problems and respond quickly.

Each large company or university that subscribes to the Internet must have an intermediate level of network organisation and expertise. A half dozen routers might be configured to connect several dozen departmental LANs in several buildings. All traffic outside the organisation would typically be routed to a single connection to a regional network provider.

However, the end user can install TCP/IP on a personal computer without any knowledge of either the corporate or regional network. Three pieces of information are required:

1 The IP address assigned to this personal computer.

2 The part of the IP address (the subnet mask) that distinguishes other machines on the same LAN (messages can be sent to them directly) from machines in other departments or elsewhere in the world (which are sent to a router machine)

3 The IP address of the router machine that connects this LAN to the rest of the world.

Transmission media and network components

Objectives : At the end of this lesson you shall be able to
- **explain cable media, wireless media and network adapter.**

Network media : Media are what the message is transmitted over. Different media have different properties and are most effectively used in different environments for different purposes.

In computer networking, the medium affects nearly every aspect of communication. Most important, it determines how quickly and to whom a computer can talk and how expensive the process is.

Cable media : Cables have a central conductor that consists of a wire or fiber surrounded by a plastic jacket. Three types of cable media are twisted-pair, coaxial and fiber-optic cable. Two types of twisted-pair cable are used in networks: unshielded (UTP) and shielded (STP).

Table summarizes the characteristics of these types of cable media, which are discussed in the following sections.

Factor	UTP	STP	Coaxial	Fiber-optic
Cost	Lowest	Moderate	Moderate	Highest
Installation	Easy	Fairly easy	Fairly easy	Difficult
Bandwidth capacity	1- to 155 Mbps (typically 10 Mbps)	1- to 155Mbps (typically 16 Mbps)	Typically 10 Mbps	2 Gbps (typically 100 Mbps)
Node capacity per segment	2	2	30 (10base 2) 100 (10 base 5)	2
Attenuation	High (range of hundreds of meters)	High (range of hundreds of meters)	Lower (range of a few kilometers)	Lowest (range of tens of kilometers)
EMI	Most vulnerable to EMI and eavesdropping	Less vulnerable than UTP but still vulnerable to EMI and eavesdropping	Less vulnerable than UTP but still vulnerable to EMI and eavesdropping	Not affected by EMI or eavesdropping

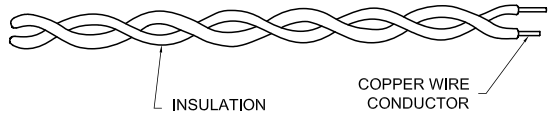
Twisted-pair cable : Twisted-pair cable uses one or more pairs of two twisted copper wires to transmit signals. It is commonly used as telecommunications cable.

When copper wires that are close together conduct electric signals, there is a tendency for each wire to produce interference in the other. One wire interferring with another in this way is called crosstalk. To decrease the amount of crosstalk and outside interference, the wires are twisted. Twisting the wires allows the emitted signals from one wire to cancel out the emitted signals from the other and protects them from outside noise.

Twisted pairs are two color-coded, insulated copper wires that are twisted around each other. A twisted-pair cable consists of one or more twisted pairs in a common jacket. Fig 1 shows a twisted-pair cable.

The two types of twisted-pair cable are unshielded and shielded.

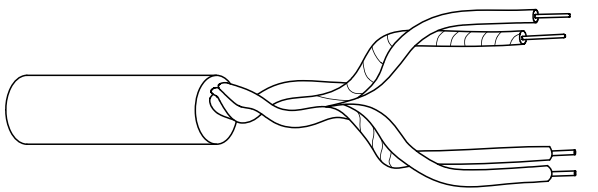
Fig 1



Unshielded twisted-pair cable : Unshielded twisted-pair (UTP) cable consists of a number of twisted pairs with a simple plastic casing. UTP is commonly used in telephone systems. Fig 2 shows a UTP cable.

The Electrical Industries Association (EIA) divides UTP into different categories by quality grade. The rating for each category refers to conductor size, electrical characteristics and twists per foot. The following categories are defined.

Fig 2

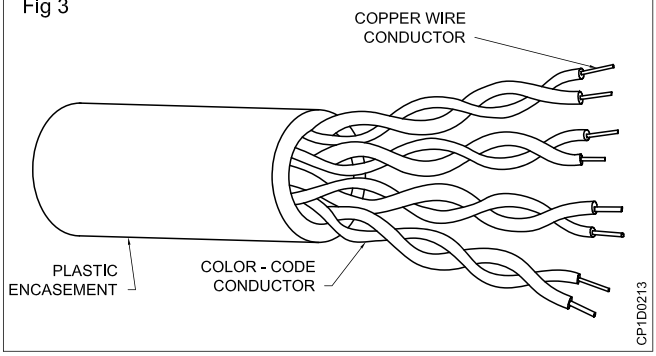


CP1D0212

– Categories 1 and 2 were originally meant for voice communication and can support only low data rates, less than 4 megabits per second (Mbps). These cannot be used for high-speed data communications. Older telephone networks used Category 1 cable.
– Category 3 is suitable for most computer networks. Some innovations can allow data rates much higher, but generally Category 3 offers data rates up to 16 Mbps. This category of cable is the kind currently used in most telephone installations.
– Category 4 offers data rates upto 20 Mbps.
– Category 5 offers enhancements over Category 3, such as support for Fast Ethernet, more insulation and more twists per foot, but Category 5 requires compatible equipment and more stringent installation. In a Category 5 installation, all media, connectors and connecting equipment must support Category 5 or performance will be affected.

Data-grade UTP cable (Categories 3,4 and 5) consists of either four or eight wires. A UTP cable with four wires is called a two-pair. Network topologies that use UTP require atleast two-pair wire. You may want to include an extra pair for future expansion. Fig 3 shows a four-pair cable.

Fig 3



CP1D0213

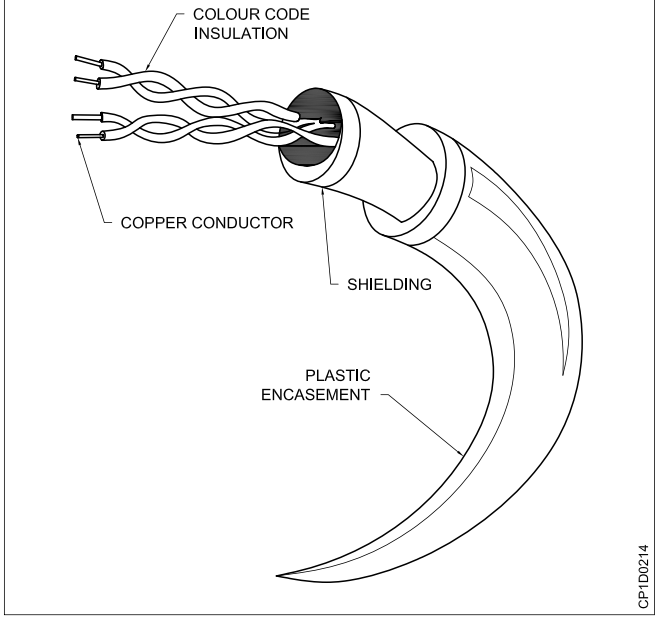
Because UTP cable was originally used in telephone systems, UTP installations are often similar to telephone installations. For a four-pair cable, you need a modular RJ-45 telephone connector. For a two-pair cable, you need a modular RJ-11 telephone connector. These connectors are attached to both ends of a patch cable. One end of the patch cable is then inserted into a computer or other device, and the other end is inserted into a wall jack. The wall jack connects the UTP drop cable (another length of cable) to a punch-down block.

The other side of the punch-down block is wired to a patch panel. The patch panel provides connectivity through patch cables to other user devices and connectivity devices.

UTP's popularity is partly due to the, first usage of the same in telephone systems. In many cases a network can be run over the already existing wires installed for the phone system, at a great savings in installation cost.

Shielded twisted-pair cable : The only difference between shielded twisted pair (STP) and UTP is that STP cable has a shielded usually aluminium/polyester between the outer jacket or casing and the wires. Fig 4 shows STP cable.

Fig 4



CP1D0214

The shield makes STP less vulnerable to EMI because the shield is electrically grounded. If a shield is grounded correctly, it tends to prevent signals from getting into or out of the cable. It is a more reliable cable for LAN environments. STP was the first twisted-pair cable to be used in LANs. Although many LANs now use UTP, STP is still used.

Transmission media specifications from IBM and Apple Computer use STP cable. IBM's Token Ring network uses STP and IBM has its own specifications for different qualities and configurations of STP. A completely different type of STP is the standard for Apple's Apple Talk networks. Networks that confirm to each vendor's specifications have their own special requirements, including connector types and limits on cable length.

STP has the following characteristics

Cost : Bulk STP is fairly expensive. STP costs more than UTP and thin coaxial cable but less than thick coaxial or fiber-optic cabling.

Installation : The requirement for special connectors can make STP more difficult to install than UTP. An electrical ground must be created with the connectors. To simplify installation, use standardised and prewired cables.

Because STP is rigid and thick (up to 1.5 inches in diameter), it can be difficult to handle.

Bandwidth capacity : With the outside interference reduced by the shielding, STP can theoretically run at 500 Mbps for a 100 meter cable length. Few installations run at data rates higher than 155 Mbps. Currently, most STP installations have data rates of 16 Mbps.

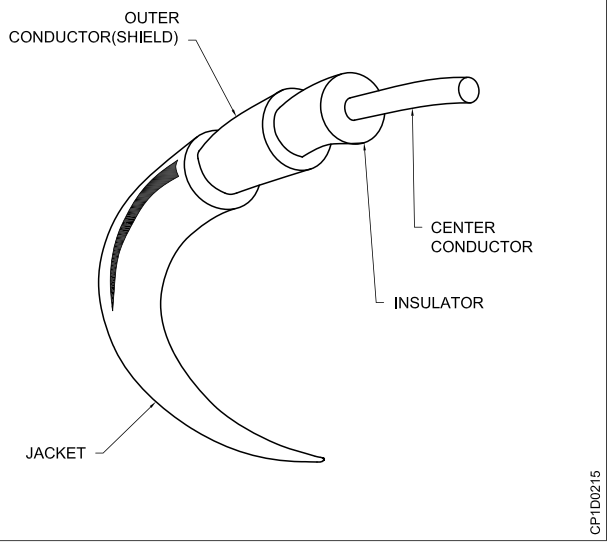
Node capacity : Since only two computers can be connected together by an STP cable, the number of computers in an STP network is not limited by the cable. Rather, it is limited by the hub or hubs that connect the cables together. In a Token Ring network, which is the most common type of STP network, the useful upper limit is around 200 nodes in a single ring, but it depends on the type of data traffic in your network. There is a specified maximum limit of 270, but you will probably never reach this limit.

Attenuation : STP does not outperform UTP by much in terms of attenuation. The most common limit is 100 meters.

EMI : The biggest different between STP and UTP is the reduction of EMI. The shielding blocks a considerable amount of the interference. However, since it is copper wire, STP still suffers from EMI and is vulnerable to eavesdropping.

Coaxial cable : Coaxial cable commonly called coax has two conductors that share the same axis. A solid copper wire or stranded wire runs down the center of the cable and this wire is surrounded by plastic foam insulation. The form is surrounded by a second conductor, a wire mesh tube, metallic foil or both. The wire mesh protects the wire from EMI. It is often called the shield. A tough plastic jacket forms the cover of the cable, providing protection and insulation. Fig 5 shows a coaxial cable.

Fig 5



Coaxial cable comes in different sizes. It is classified by size (RG) and by the cable's resistance to direct or alternating electric currents (measured in ohms also called impedance)

The following are some coaxial cables commonly used in networking:

50 ohm, RG-8 and RG-11 used for thick ethernet.

50 ohm, RG-58 used for thin ethernet.

75 ohm, RG-59 used for cable TV.

93 ohm, RG-62 used for ARCnet.

PVC and plenum cable : Polyvinyl chloride (PVC) is commonly used in coaxial cabling because it is a flexible, inexpensive plastic well suited for use as insulation and cable jacketing. PVC is often used in the exposed areas of an office.

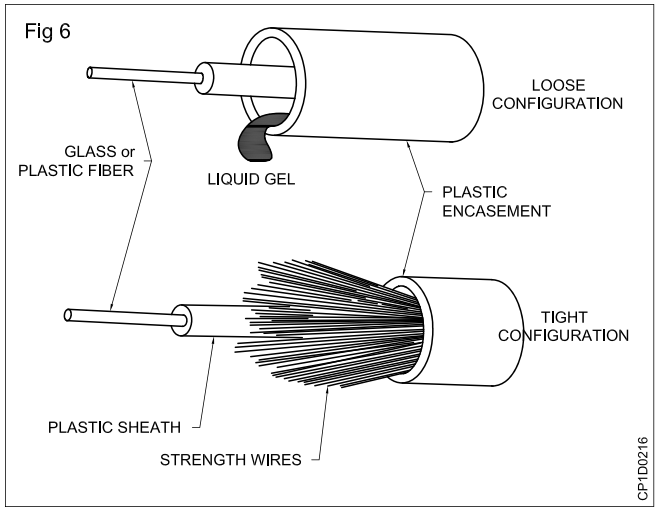
A plenum is the space between the false ceiling of an office and the floor above. The air in the plenum circulates with the air in the rest of the building, and there are strict fire codes about what can be placed in a plenum environment.

Because PVC gives off poisonous gases when burned, you cannot use it in a plenum environment. You must use plenum grade cable instead. Plenum grade cable is certified to be fire resistant to produce a minimum amount of smoke. Plenum cable is also used in vertical runs (walls) without conduit (a tube to hold the cable). Plenum cable is more expensive and less flexible than PVC.

Fiber-optic cable : Fiber-optic cable transmits light signals rather than electrical signals. It is enormously more efficient than the other network transmission media. As soon as it comes down in price (both in terms of the cable and installation costs) fibre optic will be the choice for network cabling.

Each fiber has an inner core of glass or plastic that conducts light. The inner core is surrounded by cladding, a layer of glass that reflects the light back into the core. Each fiber is surrounded by a plastic sheath. The sheath can be either tight or loose. Fig 6 shows examples of these two types of fiber optic cables.

Fig 6



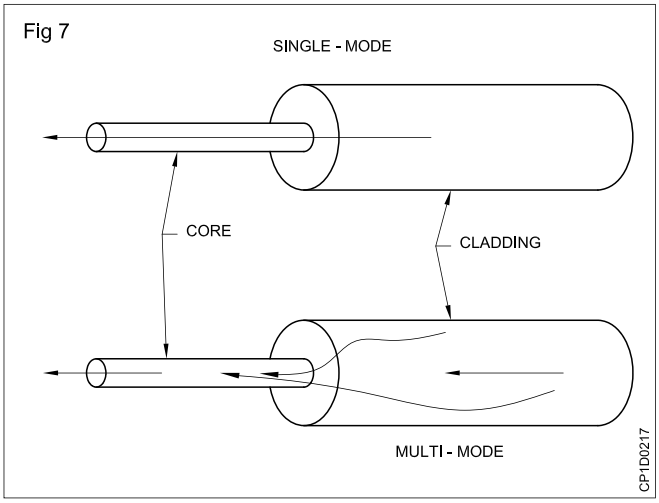
Tight configurations completely surround the fibers with a plastic sheath and sometimes include wires to strengthen the cable (although these wires are not required). Loose configurations leave a space between the sheath and the

outer jacket, which is filled with a gel or other material. The sheath provides the strength necessary to protect against breaking or extreme heat or cold. The gel, strength wires and outer jacket provide extra protection.

A cable may contain a single fiber, but often fibers are bundled together in the center of the cable. Optical fibers are smaller and lighter than copper wire. One optical fiber is approximately the same diameter as a human hair.

Optical fibers may be multimode or single mode. Single mode fibers allow a single light path and are typically used with laser signaling. Single mode fiber can allow greater bandwidth and cable runs than multimode but is more expensive. Multimode fibers use multiple light paths. The physical characteristics of the multimode fiber make all parts of the signal (those from the various paths) arrive at the same time, appearing to the receiver as though they were one pulse. If you want to save money, look into multimode, since it can be used with LEDs (light emitting diodes) which are a more affordable light source than lasers. Fig 7 shows single mode and multi mode fibers.

Fig 7



Optical fibers are differentiated by core/cladding size and mode. The size and purity of the core determine the amount of light that can be transmitted. The following are the common types of fiber-optic cable.

8.3 micron core/125 micron cladding, single mode

62.5 micron core/125 micron cladding, multimode

50 micron core/125 micron cladding, multimode

100 micron core/140 micron cladding, multimode

A typical LAN installation starts at a computer or network device that has a fiber-optic network interface and (NIC). This NIC has an incoming interface and an outgoing interface. The interfaces are directly connected to fiber-optic cables with special fibre-optic connectors. The opposite ends of the cables are attached to a connectivity device or splice center.

Wireless media : Wireless media do not use an electrical or optical conductor. In most cases, the earth's atmosphere is the physical path for the data. Wireless media is therefore useful when distance or obstructions make bounded media difficult. There are three main types of wireless media: radio wave, micro wave and infrared.

Radio wave transmission systems : Radio waves have frequencies between 10 kilohertz (KHz) and 1 gigahertz (GHz). The range of the electromagnetic spectrum between 10 KHz and 1 GHz is called radio frequency (RF).

Radio wave include the following types.

Short wave

Very high frequency (VHF) television and FM radio

Ultra-high frequency (UHF) radio and television

Radio waves can be broadcast omnidirectionally or directionally. Various kinds of antennas can be used to broadcast radio signals.

Microwave transmission systems : Microwave communication makes use of the lower gigahertz frequencies of the electromagnetic spectrum. These frequencies, which are higher than radio frequencies, produce better throughout and performance. There are two types of microwave data communication systems: terrestrial and satellite.

Terrestrial microwave : Terrestrial microwave systems typically use directional parabolic antennas to send and receive signals in the lower gigahertz range. The signals are highly focused and the physical path must be line-of-sight. Relay towers are used to extend signals. Terrestrial microwave systems are typically used when using cabling is cost prohibitive.

Because terrestrial microwave equipment often uses licensed frequencies, additional costs and time constraints may be imposed by licensing commissions or government agencies (the FCC, in the United States).

Fig 8

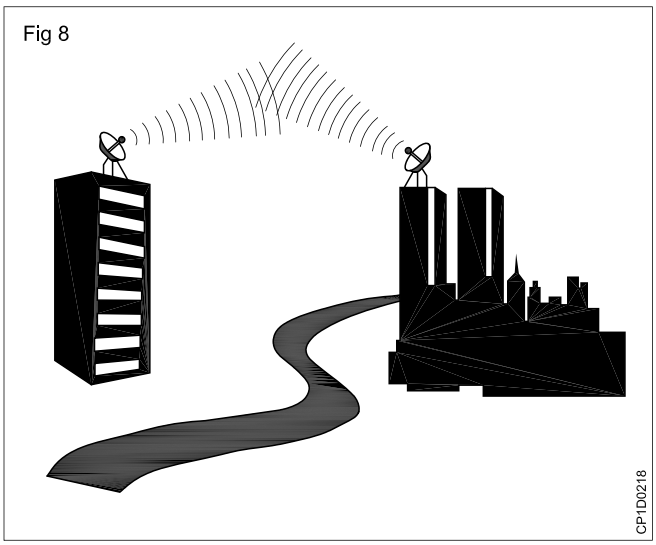


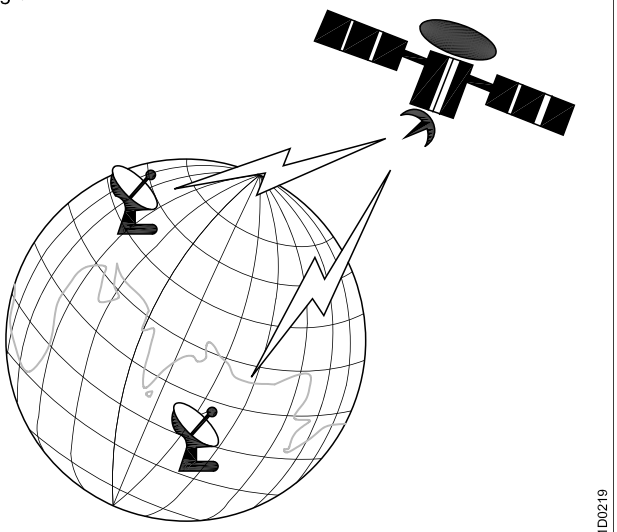
Fig 8 shows a microwave system connecting separate buildings. Smaller terrestrial microwave systems can be used within a building, as well. Microwave LANs operate at low power, using small transmitters that communicate with omnidirectional hubs. Hubs can then be connected to form an entire network.

Satellite : Satellite microwave systems transmit signals between directional parabolic antennas. Like terrestrial microwave systems, they use low gigahertz frequencies and must be in line-of-sight. The main difference with satellite system is that one antenna is on a satellite in geosynchronous orbit about 50,000 kilometers (22,300 miles) above the earth. Because of this, satellite microwave systems can reach the most remote places on earth and communicate with mobile devices.

Here's how it usually works: a LAN sends a signal through cable media to an antenna (commonly known as a satellite dish), which beams the signal to the satellite in orbit above the earth. The orbiting antenna then transmits the signal to the another location on the earth or, if the destination is on the opposite side of the earth, to another satellite, which then transmits to a location on earth.

Fig 9 shows a transmission being learned from a satellite dish on earth to an orbiting satellite and then back to earth.

Fig 9



Because the signal must be transmitted 50,000 kilometers to the satellite and 50,000 kilometers back to earth, satellite microwave transmissions take about as long to cover a few kilometers as they do to span continents. Because the transmission must travel long distances, satellite microwave systems experience delays between the transmission of a signal and its reception. These delays are called propagation delays. Propagation delays range from .5 to 5 seconds.

Infrared transmission systems : Infrared media use infrared light to transmit signals. LEDs or ILDs transmit the signals and photodiodes receive the signals. Infrared media use the tera-hertz range of the electromagnetic spectrum. The remote controls we use for television, VCR and CD players use infrared technology to send and receive signals.

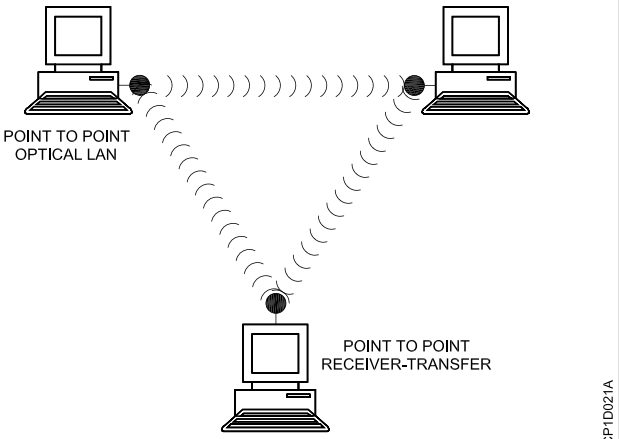
Because infrared signals are in the terahertz (higher-frequency) range, they have good throughout. Infrared signals do have a downside: the signals cannot penetrate walls or other objects and they are diluted by strong light sources.

Infrared media use pure light, normally containing only electromagnetic waves or photons from a small range of the electromagnetic spectrum. Infrared light is transmitted either line-of-sight (point-to-point) or broadcast omnidirectionally, allowing it to reflect off walls and ceilings. Point-to-point transmission allows for better data rates, but devices must remain in their locations. Broadcast, on the other hand, allows for more flexibility but with lower data rates. (Part of the signal strength is lost with each reflection.)

Point-to-point : Infrared beams can be tightly focused and directed at a specific target. Laser transmitters can transmit line-of-sight across several thousand meters.

One advantage of infrared is that an FCC license is not required to use it. Also, using point-to-point infrared media reduces attenuation and makes eavesdropping difficult. Typical point-to-point infrared computer equipment is similar to that used for consumer product with remote controls. Careful alignment of transmitter and receiver is required. Fig 10 shows how a network might use point-to-point infrared transmission.

Fig 10



Broadcast : Broadcast infrared systems spread the signal to cover a wider area and allow reception of the signal by several receivers. One of the major advantage is mobility; the workstations or other devices can be moved more easily than with point-to-point infrared media. Fig 11 shows how a broadcast infrared system might be used.

Because broadcast infrared signals are not as focussed as point-to-point, this type of system cannot offer the same throughout. Broadcast infrared is typically limited to less than 1 Mbps, making it too slow for most network needs.

Network adapters, sometimes called Network Interface Cards (NICs) are peripheral cards that plug into the motherboard of your computer and into a network cable. It is through the network adapter that your computer communicates on the network. Many newer IBM-compatible computers have built-in networking adapters for Ethernet.

Network adapters perform all the functions required to communicate on a network. They convert data from the

form stored in the computer to the form transmitted or received (or transceived) on the cable and provide a physical connection to the network.

Fig 11

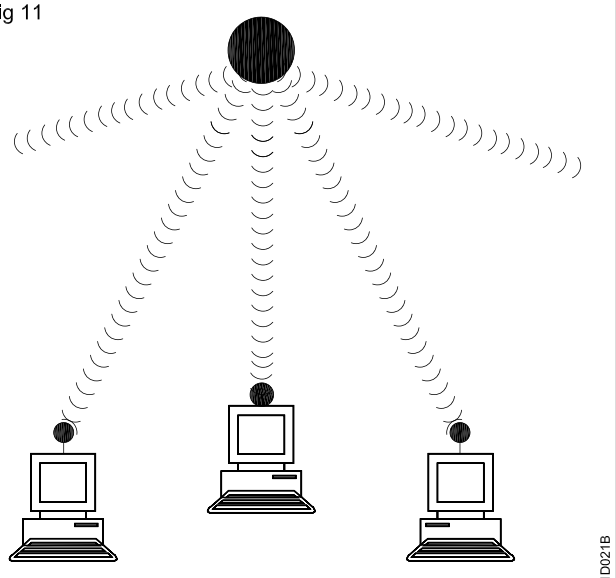
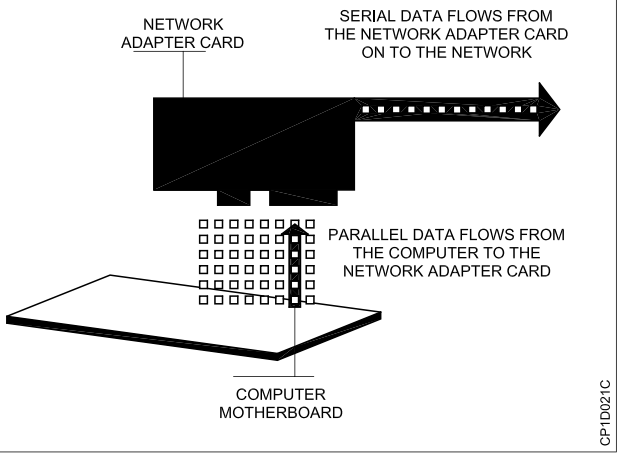


Fig 12 shows how an adapter plugs into a computer and attaches to a network cable.

Fig 12



Adapters in Abstract : Your computer software does not have to be aware of how the network adapter performs its function because the network driver software handles all the specifics for your computer. The applications running on your computer need only address data and hand it to the adapter card.

This is much the way the post office or a parcel delivery service works. You don't care about the details of postal delivery; you simply address your parcel and hand it to the delivery driver. The postal service manages the process of delivering it for you.

This abstraction allows your computer to use a microwave radio transmitter just as earily as a fiber-optic network adapter or an adapter that works over coaxial cable.

Everything in your computer remains the same except for the actual network adapter and the driver software for that adapter.

How network adapters work : Network adapters receive the data to be transmitted from the motherboard of your computer into a small amount of RAM called a buffer. The data in the buffer is moved into a chip that calculates a checksum value for the chunk and adds address information, which includes the address of the destination card and its own address, which indicates where the data is from. Ethernet adapter addresses are permanently assigned when the adapter is made at the factory. This chunk is now referred to as a frame.

For example, in Ethernet, the adapter listens for silence on the network when no other adapters are transmitting. It then begins transmitting the frame one bit at a time, starting with the address information, then the chunk of data and then the checksum.

The network adapter must still convert the serial bits of data to the appropriate media in use on the network. For instance, if the data is being transmitted over optical fiber, the bits are used to light up an infrared LED (light emitting diode) or laser diode, which transmits light pulses down the fiber to the receiving device's APD (avalanche photo diode) or photo-transistor. If the data is being sent over twisted-pair cable, the adapter must convert the bits of data from the 5-volt logic used in computers to the differential logic used for digital twisted-pair transmission.

The circuitry used to perform this media conversion is called a transceiver. Ethernet is the same no matter what type of media you use only the transceiver changes. Transceivers can be external devices attached through the AUI port on an Ethernet adapter, or they can be internal on the card. Some cards (usually called combo cards) have more than one type of transceiver built in so you can use them with your choice of media. AUI interfaces on Ethernet adapters are not transceivers-they are where you attach a transceiver for the different media types.

Because a network signal travels through copper and optical fiber at about 66 percent as fast as the speed of light, there's a chance that one of two adapters far away from each other could still be hearing silence when the other has in fact started transmitting. In this case, they could transmit simultaneously and garble their data. This is referred to as a collision.

While adapters transmit, they listen to the wire to make sure the data on the line matches the data being transmitted. As long as it does, everything is fine. If another adapter has interrupted, the data being, "heard" by the transmitting network adapter will not match the data being transmitted. If this happens, the adapter ceases transmitting and transmits a solid on state instead, which indicates to all computers that it has detected a collision and that they should discard the current frame because it has been corrupted. The network adapter waits a random amount of time and then again attempts to transmit the frame.

Configuring network adapters : Because network adapters have not been around since computers were invented, there is no assigned place for cards to be set to. Most adapter cards require their own interrupt, port address and upper memory range. PCI motherboards automatically assign IRQ and post settings to your PCI card, so you don't need to worry about it.

Unfortunately, network adapters in computers with ISA buses can conflict with other devices, since no two devices should share the same interrupt or port. No software that comes with your computer will tell you every interrupt and port in use unless your computer is already running Windows NT, so you must be somewhat familiar with the hardware in your computer or use a program that can probe for free resources to find one. Many adapters have test programs that can tell you whether the adapter is working correctly with the settings you've assigned.

Computer name and workgroup - Client server

Objectives : At the end of this lesson you shall be able to

- **define computer name**
- **define workgroup**
- **explain client-server model, centralised computing and client computing with central file storage**
- **explain web server.**

Computer Name: In network computers are identified by its IP Address, but a name can also be given to identify it easily as remembering IP address is difficult comparing remembering a alphanumeric name.

Client-Server : The term Client-Server can describe hardware, in which case it is referring to network servers and client computers, or it can refer to a way of organising software applications and services on a network. Client-server computing is a powerful way of constructing programs on a network. In order to describe its advantage and how it works, we will first describe two alternatives to client-server computing:

– Centralised computing

– Client computing with central file storage

Centralized computing : Centralized computing originated with mainframe computers and time-sharing. The principle behind centralized computing is that a central computer executes a program, such as a database or a transaction-processing program (for instance, an airline reservations system or a bank records program) and remote terminals merely display data on a screen and convey keyboard data back to the central computer.

In modern networks, personal computers can perform the role of dumb terminals. With Windows software, the PC can appear to the central computer as many terminals, each virtual terminal accessing different data or performing a separate transaction on the mainframe.

In centralized computing it is the central computer that does all the work. The data resides on the central computer and the program executes on the central computer. The personal computer or dumb terminal only display screen data and accepts keystrokes for the central computer to process. Centralized computing does not fully use the capabilities of today's powerful network clients. Fig 1 illustrates centralized computing.

Client computing with Central file storage : At the opposite end of the spectrum from centralized computing is client computing with central file storage (see Fig 2). In this way of organizing an application, the client computer does all the work. A central file server stores, but that is all.

Workgroup: In a network computers can be grouped together by using workgroup feature. Computers in a particular workgroup will show together when you open a workgroup. Though a computer of one workgroup can access other workgroup computers also.

Client computers cooperate to ensure that central files are not corrupted by attempts by several computers to access them at the same time. When a client computer needs to perform an operation, the file is transferred to the client computer to perform the operation. Two examples of this type of application are networked database programs that do not use a SQL. (Structured Query Language) server and any network-aware application that does not communicate with a special program executing on the server, such as network scheduling programs and groupware.

Fig 1

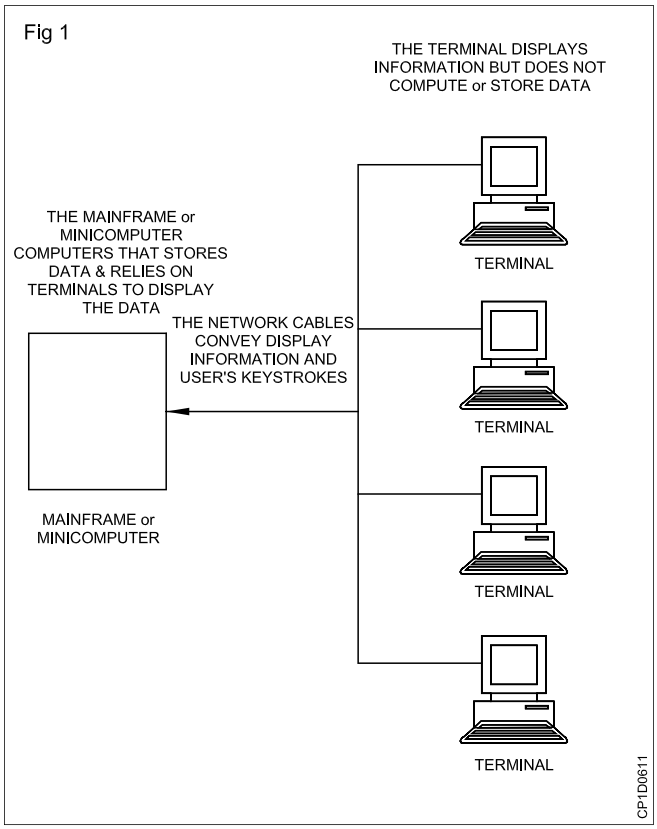
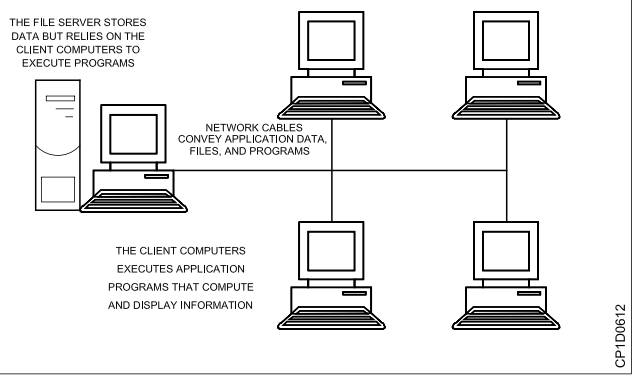


Fig 2

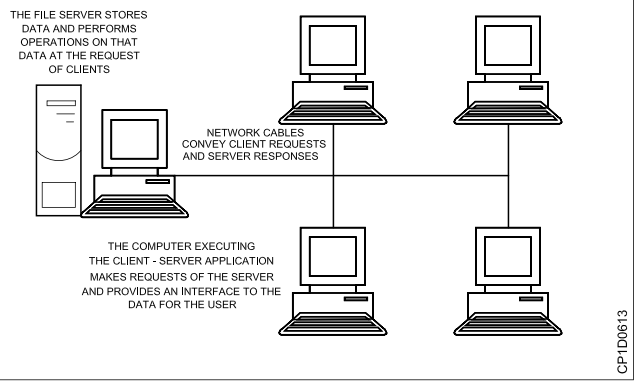


While it is fully exploits the capabilities of client computers and provides a richer and more customizable environment for the user, this type of program can place heavy demands on the network if the data files in which program works with are large. It also takes time to transmit data from the server to the client, process the data, and transfer it back to the server so other network programs can access the data.

The Client-Server Model : The client-server model combines the advantages of both the centralized computing model and the client model of computing. It does this by performing the operations that are best executed by a central computer on the file server and performing those operations that are best done close to the user on the client computer (see Fig 3). The client-server model works best when many people need access to large amounts of data. Simply stated, a client-server system is any system in which the client computer makes a request over a network to a server computer that then satisfies the request.

The Client : When you use a client-server system, what you see is the client, or front end. It presents the interface to manipulate or search for data. The request you make by manipulating windows, menu, check boxes and so on, is translated into a compact form that the client transmits over the network for the server to perform.

Fig 3



One example of a front end is Microsoft Access when it is used with a SQL back end. (You can also use Access without a SQL back end.) Access displays tables in windows or in forms you can browse. It allows you to modify and search the tables in an easy-to-use graphical environment. All the actual data manipulation, however, occurs on the SQL server. Access translates all the data-base operations into SQL for the server to perform. The results of the operations are transmitted back to Access to display in an intuitive, graphical form.

SQL is not limited to database programs such as Microsoft Access. User programs such as Microsoft Excel can use SQL to query the back-end data-base server for values to use in spreadsheet calculations. Program tools allow custom programs to store and retrieve data in server-based databases. Query tools provide direct access to the SQL data.

The Server : The server is where data operations in a client-server system occur. The central computer can service many client requests quickly and efficiently, which is the traditional advantage of centralized computing. The central computer can also provide enhanced security by performing only authorized operations on the data.

Back-end database software is optimized to perform searches and sorts and the back-end computer is often more powerful than the front-end computer.

Web server : A web server is a program using the client/ server model and the World Wide Web's Hyper Text Transfer Protocol (HTTP) serves the files that form web pages to web users.

Every computer on the internet that contains a web site must have a web server program. The most popular web servers are: The Microsoft's Internet Information Server (IIS) which comes with the Microsoft's Windows NT Server; Netscape Fast Track and Enterprises Servers and Apache, a web server for Unix-based operating systems. Other web servers include Novell's Web Server for users of its Netware Operating System and IBM's family of Lotus Domino Servers. Primarily for IBM's OS/ 390 and AS/400 customers.

Web servers often come as a part of a larger package of Internet related programs for serving e-mail, downloading requests for File Transfer Protocol (FTP) files and building and publishing web pages. Consideration in choosing a web server include how well it works with the operating system and other servers, its ability to handle server side programming and publishing, search engine and site building tools that may come with it.

DHCP

Objectives : At the end of this lesson you shall be able to
• define DHCP
• explain DHCP.

DHCP: Dynamic Host Control Protocol allows server computers to distribute dynamic IP address when the client establish connection to server. The server maintains a IP address pool and it offer some IP which is not already alloted to some other client. When client disconnects from server its IP then becomes free again and can be given to other client.

It is dynamic as same client can get different IP in different times. It is beneficial as requirement of IP address is less a all the clients are not always connected to server and its saves the time to allocate IP to each client manually.

Dynamic Host Configuration Protocol (DHCP) is a standard protocol defined by RFC 1541 (which is superseded by RFC 2131) that allows a server to dynamically distribute IP addressing and configuration information to clients. Normally the DHCP server provides the client with at least this basic information:

- IP Address
- Subnet Mask
- Default Gateway

Other information can be provided as well, such as Domain Name Service (DNS) server addresses and Windows Internet Name Service (WINS) server addresses. The system administrator configures the DHCP server with the options that are parsed out to the client.

Concept of proxy server

Objectives : At the end of this lesson you shall be able to
- **explain the meaning of proxy server**
- **explain common connection point**
- **explain packet filtering, domain filtering and control user access by service**
- **explain logging and web publising.**

What is a proxy server? To be a "proxy" means to act on behalf of another. This is exactly what a proxy server does; it acts on behalf of its proxy clients to interact with other servers. You could say that a proxy server is a "mediator" for computer communications.

Placing a proxy server on your network gives you several advantages, including security enhancements, coaching enhancements and greater control over your network users. The advantages of using Microsoft Proxy Server (MPS) is listed below:

– Common connection point

– Caching

– Packet filtering

– Domain filtering

– Control user access by service

– Logging

– Web publishing

Common connection point : MPS was designed to connect two networks, rather like a gateway. Typically, MPS connects an internal network and the Internet. This configuration gives the internal computers a common connection point to the Internet-through MPS.

When used to provide a common connection, MPS lets clients share a single connection to the Internet. Instead of giving each user on a Local Area Network (LAN) a separate modem, phone line and dial-up account to the Internet, MPS can function as a gateway to the Internet using a single connection. Instead of using separate standard phone line connections, users can share a single higher-speed connection through the proxy server. The net effect is usually an overall cost savings and reduction in administrative overhead. One connection is usually cheaper and easier to maintain than several separate connections.

Caching : Since you can use MPS as a common connection point to the Internet, you can also use it to cache frequently accessed resources. MPS allocates a portion of the server's hard disk space to store frequently accessed objects.

Caching can either be passive or active. Passive caching just stores objects as they are requested so the cache is updated only when users request information. Active caching directs the server to refresh objects in the cache automatically.

You can selectively control MPS caching so that you can limit the size of cached objects, change the expiration limits (control the freshness of objects) and determine whether MPS always caches or always excludes from cache certain content.

Caching only works with the Web Proxy Service in MPS. You will learn more about the Web Proxy Service later in this chapter.

Packet Filtering : To protect internal users from the outside world (in other words to protect the network from outsiders), MPS provides packet-filtering services. A packet filter prevents unauthorized access from the outside by limiting the available connection points coming into the network. To that end, packet filters stop various types of protocols from entering the network.

MPS supports both static and dynamix packet filters. A static filter keeps all traffic of a certain description or type from passing through MPServer. A dynamic packet filter automatically determines which type of traffic is allowed in or out. With a static filter the administrator defines the port, the protocol and may be the IP address. With a dynamic filter the administrator just defines the service to be allowed or filtered.

Domain Filtering : MPS also lets you limit the access of your internal clients to the Internet. You can configure filters for a single computer, a group of computers or a domain name. Many companies prefer to have this type of control over their users because they can block access to Internet sites that they believe reduce employee productivity or contain offensive material. Some popular examples of domain filtering are blocking access to Internet game servers or Web sites that contain pornographic material.

You can configure domain filters for a specific IP address, IP address and subnet mask or domain name. IP address filters prevent users from contacting a single computer. Using the IP address and subnet mask as a filter limits access to an entire group (a subnet) of computers. Domain name filters can apply to an entire Web site or to subsections of that site.

Control user access by Protocol or Service : You can also selectively enable and disable ports, services and protocols through MPS. MPS lets you control access to Internet services at the user level. You can also enable or restrict access to protocols on a user or group basis. Many protocols are predefined in the default MPS configuration.

If the protocol or service you would like to enable or disable is not defined in the MPS property sheets, you can create a new sheet. you can define a protocol by TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) port number or range. This gives you the ability to control access by port.

Logging : Because all traffic between networks passes through MPS, MPS has the unique opportunity to log and track communication. You can track the information your internal clients get from other networks or the Internet and monitor inbound communication. You can use this information to help you secure your internal network from attack and unauthorized access. Plus, you can monitor where your users spend their time on the Internet and what information they are downloading.

Web publishing : MPS can also act as a Web server. MPS can service requests from cache on behalf of a Web server, pass requests to the Web server on the local system or pass requests to another Web server on the internal network. The terms "reverse proxying" and "reverse hosting" describe the Web Publishing services that MPS provides.

As a reverse proxy, MPS listens to incoming Web requests for a single Web server on the local network. The incoming requests are simply forwarded to another Web server. Web hosting requires more work on the part of MPS. As a reverse host, MPS can send requests to one of many Web servers. In this case, MPS responds as if the entire site were contained locally, even though the actual data may be coming from several different Web servers.

The main difference between reverse proxying and reverse hosting is that in performing reverse proxying, MPS forwards all requests to the Web server. In performing reverse hosting, MPS selectively forwards requests to multiple Web servers on the internal network. In reverse hosting, the Microsoft Proxy Server routes an external request for a resource (that specifies an Internet domain name) to one or more internal Web servers. For instance, requests for http://www.hudlogic.com/bios might be routed to an internal server named "business" (http://business), while requests for http://www.hudlogic.com/pictures could be sent to a different Web server named "server1" (http://server1).

Services : Microsoft Proxy Server 2.0 supports Hypertext Transfer Protocol (HTTP) version 1.1, Windows Sockets version 1.1, SOCKS version 4.3a and Secure Sockets Layer (SSL) 3.0. The MPS services that provide this support are the Web Proxy service, WinSock Proxy service and the SOCKS Proxy service, respectively.

Web Proxy Service : The Web Proxy service provides support for HTTP (a.k.a.Web publishing), FTP, Gopher and secure (SSL) communications. The Web Proxy service works with any CERN-compliant Web browser, such as Internet Explorer or Netscape Navigator. Because the Web Proxy supports only these widely adopted Internet standard communication methods, it isn't operating system dependent. Clients running Unix, Macintosh or Windows operating systems can communicate with the Web Proxy service as long as they're configured with a CERN-complaint Web browser.

Any operating system using a CERN-compliant Web browser can communicate through the Web Proxy server, regardless of its underlying operating system.

WinSock Proxy Service : The WinSock Proxy service supports Microsoft Windows operating systems using Windows Sockets. This supprt is available for both Transmission Control Protocol/internet Protocol (TCP/IP) and Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) protocols. The WinSock Proxy service applies mainly to Windows clients including Windows 3.x, windows 95 and Windows NT.

Windows Sockets is an interprocess communication mechanism derived from the Berkeley Sockets interface (originally designed for Unix systems). The Sockets interface was extended to support Windows-based clients running Microsoft implementations of TCP/IP. The name given to this Sockets interface for Windows was WinSock (for Windows Sockets).

The WinSock Proxy Service doesn't support 16-bt IPX/SPX clients such as the Windows 3.x 16-bit Netware clients.

SOCKS Proxy Service : The SOCKS Proxy service supports SOCKS version 4.3a client applications such as FTP, Gopher and Telnet. Operating systems like Macintosh and Unix can run SOCKS 4.3a and access the SOCKS Proxy service when communicating through the Microsoft Proxy Server. One limitation of the SOCKS proxy service on MPS is that it does not support UDP-based protocols.

UDP-based protocols aren't supported through the SOCKS Proxy service, but the WinSock Proxy service does support UDP for Windows clients.

Video conferencing

Objectives: At the end of this lesson you shall be able to
- **define video conferencing**
- **list the advantages of video conferencing**
- **list the disadvantages of video conferencing.**

Video Conferencing

Definition: Videoconferencing is the conduct of a conference by a set of telecommunication technologies which allow two or more remotely located teams to communicate by simultaneous two-way video and audio transmissions. It has also been called 'visual collaboration' and is a type of groupware.

Video conferencing is a very useful technique to cut down various costs as well as travel time when meetings and conferences are concerned.Video conferencing connects individuals in real time through audio and video communication over broadband networks. It enables visual meetings and collaboration on digital documents and shared presentations. New technologies allow participants to connect remotely over a network through multiple devices like laptops, desktops, smartphones and tablets.

Advantages

1 Significant Travel Savings

2 Not only is video conferencing a direct replacement for many in-person business trips, but because there is virtually no cost to add additional key employees to a virtual meeting, it is a cost effective solution.

3 Improved Communication

4 Audio conferencing and e-mail may be used for communication but there is a lack of visual connection and eye contact in these. Video conferencing allows users to successfully convey, creating essential social bonds and shared understandings.

5 Increased Productivity

6 Important meetings are shorter and more effective. But it is a well-known fact that many meetings take longer than the necessary time of the participants. Video conferencing users can save a minimum of two hours a week with the technology. The interactivity of group collaboration and document sharing greatly increases productivity.

7 Conferencing Quality

8 The present day state-of-the-art technology delivers excellent, reliable audio and video quality, making conferencing very effective and interesting too.

Disadvantages

1 Absence of Physical Presence

2 Initial installation costs

3 Not yet popular with a large size of users.

Network security

Objectives: At the end of this lesson you shall be able to
- **define network security**
- **explain network security concepts.**

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorizedaccess, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

Network security concepts

Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name -i.e. the password- this is sometimes termed one-factor authentication. With two-factor authentication, something the user needs a 'dongle', an ATM card, or a mobile phone, and with three-factor authentication, something the user needs a fingerprint or retinal scan.

Once authenticated, a firewall decides what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network.

Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware.

Encrypting the communication between two hosts using a network helps maintain privacy.

Surveillance and early-warning toolssometimes referred to as Honeypots can be employed.

Hhoneypot is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. This is similar to the police baiting a criminal and then conducting undercover surveillance.

The Foundations of Security

Security relies on the following elements:

- **Authentication**

Authentication addresses the question: who are you? It is the process of uniquely identifying the clients of your applications and services. These might be end users, other services, processes, or computers. In security parlance, authenticated clients are referred to as principals.

- **Authorization**

Authorization addresses the question: what can you do? It is the process that governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with system-level resources such as registry keys and configuration data. Operations include performing transactions such as purchasing a product, transferring money from one account to another, or increasing a customer's credit rating.

- **Auditing**

Effective auditing and logging is the key to non-repudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction. For example, in an e-commerce system, non-repudiation mechanisms are required to make sure that a consumer cannot deny ordering 100 copies of a particular book.

- **Confidentiality**

Confidentiality, also referred to as privacy, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is frequently used to enforce confidentiality. Access control lists (ACLs) are another means of enforcing confidentiality.

- **Integrity**

Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks. Integrity for data in transit is typically provided by using hashing techniques and message authentication codes.

- **Availability**

From a security perspective, availability means that systems remain available for legitimate users. The goal for many attackers with denial of service attacks is to crash an application or to make sure that it is sufficiently overwhelmed so that other users cannot access the application.Threats, Vulnerabilities, and Attacks Defined

A threat is any potential occurrence, malicious or otherwise, that could harm an asset. In other words, a threat is any bad thing that can happen to your assets.

A vulnerability is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques. Weak input validation is an example of an application layer vulnerability, which can result in input attacks.

An attack is an action that exploits a vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application or flooding a network in an attempt to deny service.

How Do You Build a Secure Web Application?

It is not possible to design and build a secure Web application until you know your threats. An increasingly important knowledge needed is about threat modeling. The purpose of threat modeling is to analyze your application's architecture and design and identify potentially vulnerable areas that may allow a user, perhaps mistakenly, or an attacker with malicious intent, to compromise your system's security.

After you know your threats, design with security in mind by applying proven security principles. You must follow secure coding techniques to develop secure, robust, and hack-resilient solutions. The design and development of application layer software must be supported by a secure network, host, and application configuration on the servers where the application software is to be deployed.