

# Network Technologies

This section covers the different protocols used on a network. In this section you will learn about MAC addresses, the OSI model, and the common network protocols such as TCP/IP, FTP, SMTP, and TFTP, for example. This section also covers TCP/UDP port functionality, network services such as DHCP, DNS, WINS, and SNMP. IP Addressing is also covered in this part along with understanding public and private networks, WAN technologies, remote access, and security protocols.

Dhcp Server

Function of TCP UDP protocols DNS NAT ICS WINS SNMP NFS SMB AFP ISDN FDDI

TCP IP model tcp ip stack MAC OSI IPX/SPX IPX SPX NetBEUI AppleTalk

Tcp ip udp ftp smtp HTTPs POP3 IMAP4 telnet SSH ICMP ARP RARP NTP SNMP SCP LDAP LPR

Ip address IPv4 IPv6 public ip private ip APIPA Static Dynamic ip classes

Network security protocols CHAP MS-CHAP PAP RADIUS RAS PPP SLIP PPPoE PPTP RDP

Star Topology ring Topology bus Topology Logical Physical mesh Topology

Factors which affect Wireless Network Range Speed Infrared Bluetooth FHSS DSSS OFDM MIMO

Main features of 802.2 Logical Link Control 802.3 Ethernet 802.5 token ring 802.11

10BaseT 10BaseF 10Base2 5-4-3 rule 10Base5 100BaseFX 100BaseT4 100BaseTX

Types of Networks LAN MAN WAN CN VPN SAN Internet Extranet Intranet

## FUNCTION OF TCP UDP PROTOCOLS DNS NAT ICS WINS SNMP NFS SMB AFP ISDN FDDI

The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are used to transmit network data to and from server and client applications. The main difference between the two protocols is that TCP

uses a connection-oriented transport, while UDP uses a connectionless type of communication. When the TCP protocol is used, a special connection is opened up between two network devices, and the channel remains open to transmit data until it is closed.

On the other hand, a UDP transmission does not make a proper connection and merely broadcasts its data to the specified network address without any verification of receipt. For certain types of applications and services, a TCP connection makes more sense, while other types are more efficiently provided by UDP communication. The advantage of TCP is that the transmission is much more reliable because it uses acknowledgement packets to ensure delivery. The advantage of UDP is that there is no connection, so it is much faster without all the checks and acknowledgements going on, but is also less reliable. In Table some common TCP/IP applications are shown with the type of protocol they use.

Protocol	Common Port
FTP (File Transfer Protocol)	20, 21
SSH (Secure Shell)	22
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name Service)	53
TFTP (Trivial File Transfer Protocol)	69
HTTP (Hypertext Transfer Protocol)	80
POP3 (Post Office Protocol version 3)	110
NNTP (Network News Transport Protocol)	119
NTP (Network Time Protocol)	123
IMAP4 (Internet Message Access Protocol version 4)	143
HTTPS (Hypertext Transfer Protocol Secure)	443

## DNS

TCP/IP networks communicate with hosts using their IP addresses. It would be very difficult for someone to have to memorize the different IP addresses for the hosts they want to connect to on the network. A Domain Name Service (DNS) makes it easier to identify a host by a domain name. A domain name uses words rather than numbers to identify Internet hosts. Suppose you want to connect to the CompTIA Web site by using your Web browser. You would enter

```
http://www.comptia.org
```

In the address bar to go to the Comp TIA Web page. [www.comptia.org](http://www.comptia.org) would be a common name used for a numerical IP address. You could use [216.119.103.72](http://216.119.103.72) instead, but [www.comptia.org](http://www.comptia.org) is easier to remember. A DNS server translates these addresses. Your Web browser asks the TCP/IP protocol to ask the DNS server for the IP address of [www.comptia.org](http://www.comptia.org). When the browser receives the address, it connects to the Web site. Remember that DNS stands for Domain Name System (or Domain Name Service) and that a DNS server translates domain names into their IP addresses.

## NAT (Network Address Translation)

NAT translates one IP address to another. This can be a source address or a destination address. Two basic implementations of NAT can be used: static and dynamic

### Static NAT

With static NAT, a manual translation is performed by an address translation device, translating one IP address to a different one. Typically, static NAT is used to translate destination IP addresses in packets as they come into your network, but you can translate source addresses also.

### Dynamic NAT

With static address translation, you need to build the translations manually. If you have 1000 devices, you need to create 1000 static entries in the address translation table, which is a lot of work. Typically,

static translation is done for inside resources that outside people want to access. When inside users access outside resources, dynamic translation is typically used. In this situation, the global address assigned to the internal user isn't that important, since outside devices don't directly connect to your internal users—they just return traffic to them that the inside user requested.

## ICS (Internet Connection Sharing)

ICS (Internet Connection Sharing) is a built-in feature of Windows 98 Second Edition, Windows 2000, Windows Me, and Windows Xp. ICS provides networked computers with the capability to share a single connection to the Internet. Multiple users can use ICS to gain access to the Internet through a single connection by using Dial-Up Networking or local networking.

## WINS (Windows Internet Name Service)

While DNS resolves host names to IP addresses, WINS resolves NetBIOS names to IP addresses. Windows Internet Name Service provides a dynamic database of IP address to NetBIOS name resolution mappings. WINS, determines the IP address associated with a particular network computer. This is called name resolution. WINS supports network client and server computers running Windows. WINS uses a distributed database that is automatically updated with the names of computers currently available and the IP address assigned to each one. DNS is an alternative for name resolution suitable for network computers with fixed IP addresses.

## SNMP (Simple Network Management Protocol)

Simple Network Management Protocol, is a TCP/IP protocol for monitoring networks and network components. SNMP uses small utility programs called agents to monitor behavior and traffic on the network, in order to gather statistical data. These agents can be loaded onto managed devices such as hubs, NIC's, servers, routers, and bridges. The gathered data is stored in a MIB (management information base). To collect the

information in a usable form, a management program console polls these agents and downloads the information from their MIB's, which then can be displayed as graphs, charts and sent to a database program to be analyzed.

## NFS (Network File System)

Network File System (NFS) is a distributed file system that allows users to access files and directories located on remote computers and treat those files and directories as if they were local.

## Zeroconf (Zero configuration)

Zero Configuration Networking is a set of techniques that automatically create a usable IP network without configuration or special servers. This allows unknowledgeable users to connect computers, networked printers, and other items together and expect them to work automatically. Without Zeroconf or something similar, a knowledgeable user must either set up special servers, like DHCP and DNS, or set up each computer's network settings manually.

### **Zeroconf currently solves three problems :**

- Choose numeric network addresses for networked items
- Figure out which computer has a certain name
- Figure out where to get services, like printing.

## SMB (Server Message Block)

A file-sharing protocol designed to allow networked computers to transparently access files that reside on remote systems over a variety of networks. The SMB protocol defines a series of commands that pass information between computers. SMB uses four message types: session control, file, printer, and message. It is mainly used by Microsoft Windows equipped computers. SMB works through a client-server approach, where a client makes specific requests and the server responds accordingly. One section of the SMB protocol is specifically for filesystem access, such that clients may make requests to a file server. The SMB protocol was

optimised for local subnet usage, but one could use it to access different subnets across the Internet on which MS Windows file-and-print sharing exploits usually focus. Client computers may have their own hard disks, which are not publicly shared, yet also want access to the shared file systems and printers on the server, and it is for this primary purpose that SMB is best known and most heavily used.

### AFP (Apple File Protocol)

The file sharing protocol used in an AppleTalk network. In order for non-Apple networks to access data in an AppleShare server, their protocols must translate into the AFP language. AFP versions 3.0 and greater rely exclusively on TCP/IP (port 548 or 427) for establishing communication, supporting AppleTalk only as a service discovery protocol. The AFP 2.x family supports both TCP/IP and AppleTalk for communication and service discovery.

### LPD (Line Printer Daemon) and Samba)

LPD is the primary UNIX printing protocol used to submit jobs to the printer. The LPR component initiates commands such as "print waiting jobs," "receive job," and "send queue state," and the LPD component in the print server responds to them. The most common implementations of **LPD** are in the official BSD UNIX operating system and the LPRng project. The Common Unix Printing System (or CUPS), which is more common on modern Linux distributions, borrows heavily from LPD. Unix and Mac OS X Servers use the Open Source **SAMBA** to provide Windows users with Server Message Block (SMB) file sharing.

## WAN (Wide Area Networks) technologies:

### Circuit-switched

services provide a temporary connection across a phone circuit. In networking, these are typically used for backup of primary circuits and for temporary boosts of bandwidth.

### dedicated circuit

dedicated circuit is a permanent connection between two sites in which the bandwidth is dedicated to that company's use. These circuits are common when a variety of services, such as voice, video, and data, must traverse the connection and you are concerned about delay issues with the traffic and guaranteed bandwidth.

### Cell-switched

cell-switched services can provide the same features that dedicated circuits offer. Their advantage over dedicated circuits is that a single device can connect to multiple devices on the same interface. The downside of these services is that they are not available at all locations, they are difficult to set up and troubleshoot, and the equipment is expensive when compared to equipment used for dedicated circuits.

### Packet switching

Packet-switched services are similar to cell-switched services. Whereas cell-switched services switch fixed-length packets called cells, packet-switched services switch variable-length packets. This feature makes them better suited for data services, but they can nonetheless provide some of the QoS features that cell-switched services provide. Packet switching offers more efficient use of a telecommunication provider's network bandwidth. With packet switching, the switching mechanisms on the network route each data packet from switch to switch individually over the network using the best-available path. Any one physical link in a packet-switched network can carry packets from many different senders and for many different destinations. Where as in a circuit switched connection, the bandwidth is dedicated to one sender and receiver only.

### ISDN (Integrated Services Digital Network)

Integrated Services Digital Network adapters can be used to send voice, data, audio, or video over standard telephone cabling. ISDN adapters must be connected directly to a digital telephone network. ISDN adapters are not actually modems, since they neither modulate nor demodulate the digital ISDN signal. Like standard modems, ISDN adapters are available

both as internal devices that connect directly to a computer's expansion bus and as external devices that connect to one of a computer's serial or parallel ports. ISDN can provide data throughput rates from 56 Kbps to 1.544 Mbps using a T1 service. ISDN hardware requires a NT (network termination) device, which converts network data signals into the signaling protocols used by ISDN. Some times, the NT interface is included, or integrated, with ISDN adapters and ISDN-compatible routers. In other cases, an NT device separate from the adapter or router must be implemented. ISDN works at the physical, data link, network, and transport layers of the OSI Model.

### FDDI (Fiber Distributed Data Interface)

Fiber Distributed Data Interface, shares many of the same features as token ring, such as a token passing, and the continuous network loop configuration. But FDDI has better fault tolerance because of its use of a dual, counter-rotating ring that enables the ring to reconfigure itself in case of a link failure. FDDI also has higher transfer speeds, 100 Mbps for FDDI, compared to 4 - 16 Mbps for Token Ring. Unlike Token Ring, which uses a star topology, FDDI uses a physical ring. Each device in the ring attaches to the adjacent device using a two stranded fiber optic cable. Data travels in one direction on the outer strand and in the other direction on the inner strand. When all devices attached to the dual ring are functioning properly, data travels on only one ring. FDDI transmits data on the second ring only in the event of a link failure.

Media	MAC Method	Signal Propagation Method	Speed	Topologies	Maximum Connections
Fiber-optic	Token passing	Forwarded from device to device (or port to port on a hub) in a closed loop	100 Mbps	Double ring Star	500 nodes

### T1 (T Carrier level 1)

A 1.544 Mbps point to point dedicated, digital circuit provided by the telephone companies. T1 lines are widely used for private networks as



well as interconnections between an organizations LAN and the telco. A T1 line uses two pairs of wire one to transmit, and one to receive. and time division multiplexing (TDM) to interleave 24 64-Kbps voice or data channels. The standard T1 frame is 193 bits long, which holds 24 8-bit voice samples and one synchronization bit with 8,000 frames transmitted per second. T1 is not restricted to digital voice or to 64 Kbps data streams. Channels may be combined and the total 1.544 Mbps capacity can be broken up as required.

### T3 (T Carrier level 3)

A T3 line is a super high-speed connection capable of transmitting data at a rate of 45 Mbps. A T3 line represents a bandwidth equal to about 672 regular voice-grade telephone lines, which is wide enough to transmit real time video, and very large databases over a busy network. A T3 line is typically installed as a major networking artery for large corporations, universities with high-volume network traffic and for the backbones of the major Internet service providers.

### OCx (Optical Carrier)

Optical Carrier, designations are used to specify the speed of fiber optic networks that conforms to the SONET standard.

Level	Speed
OC-1	51.85 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps

### X.25

X.25 is a network layer protocol that runs across both synchronous and asynchronous physical circuits, providing a lot of flexibility for your connection options. X.25 was actually developed to run across unreliable medium. It provides error detection and correction, as well as flow control, at both the data link layer (by LAPB) and the network layer (by X.25). In this sense, it performs a function similar to what TCP, at the transport layer, provides for IP. Because of its overhead, X.25 is best delegated to asynchronous, unreliable connections. If you have a synchronous digital connection, another protocol, such as Frame Relay or ATM, is much more efficient. An X.25 network transmits data with a packet-switching protocol, bypassing noisy telephone lines. This protocol relies on an elaborate worldwide network of packet-forwarding nodes that can participate in delivering an X.25 packet to its designated address.

## Internet access technologies:

### xDSL (Digital Subscriber Line)

xDSL is a term referring to a variety of new Digital Subscriber Line technologies. Some of these varieties are asymmetric with different data rates in the downstream and upstream directions. Others are symmetric. Downstream speeds range from 384 Kbps (or "SDSL") to 1.5-8 Mbps (or "ADSL").

### Asymmetric Digital Subscriber Line (ADSL)

A high-bandwidth digital transmission technology that uses existing phone lines and also allows voice transmissions over the same lines. Most of the traffic is transmitted downstream to the user, generally at rates of 512 Kbps to about 6 Mbps.

### Broadband Cable (Cable modem)

Cable modems use a broadband connection to the Internet through cable television infrastructure. These modems use frequencies that do not interfere with television transmission.

### POTS / PSTN

(Plain Old Telephone Service / Public Switched Telephone Network) **POTS / PSTN** use modem's, which is a device that makes it possible for computers to communicate over telephone lines. The word modem comes from Modulate and Demodulate. Because standard telephone lines use analog signals, and computers digital signals, a sending modem must modulate its digital signals into analog signals. The computers modem on the receiving end must then demodulate the analog signals into digital signals. Modems can be external, connected to the computers serial port by an RS-232 cable or internal in one of the computers expansion slots. Modems connect to the phone line using standard telephone RJ-11 connectors.

## Wireless

A wireless network consists of wireless NICs and access points. NICs come in different models including PC Card, ISA, PCI, etc. Access points act as wireless hubs to link multiple wireless NICs into a single subnet. Access points also have at least one fixed Ethernet port to allow the wireless network to be bridged to a traditional wired Ethernet network, such as the organization's network infrastructure. Wireless and wired devices can coexist on the same network.

- **WLAN (Wireless Local Area Network)** A group of computers and associated devices that communicate with each other wirelessly.
- **WPA (Wi-Fi Protected Access)** A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.
- **WPA2 (Wi-Fi Protected Access 2)** WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.
- **WPA-Personal** A version of WPA that uses long and constantly changing encryption keys to make them difficult to decode.

- **WPA-Enterprise** A version of WPA that uses the same dynamic keys as WPA-Personal and also requires each wireless device to be authorized according to a master list held in a special authentication server.

## TCP IP MODEL TCP IP STACK MAC OSI IPX/SPX IPX SPX NETBEUI APPLE TALK

A MAC address is 48 bits long and is represented as a hexadecimal number. Represented in hex, it is 12 characters in length, where each character is 4 bits. To make it easier to read, the MAC address is represented in a dotted hexadecimal format, like this: **FFFF.FFFF.FFFF.**

Some formats use a colon (:) instead; and in Some cases, the colon separator is spaced after every two hexadecimal digits, like this: **FF:FF:FF:FF:FF:FF.** the first six digits of a MAC address are associated with the vendor, or maker, of the NIC.

Each vendor has one or more unique sets of six digits. These first six digits are commonly called the **organizationally unique identifier (OUI)**. The last six digits are used to represent the NIC uniquely within the OUI value. In theory, each NIC has a unique MAC address. In reality however, this is probably not true. What is important for your purposes is that each of your NICs has a unique MAC address within the same physical or logical segment.

A logical segment is a virtual LAN (VLAN) and is referred to as a broadcast domain .

Some devices, such as Cisco routers, might allow you to change the MAC address for a NIC, while others won't.

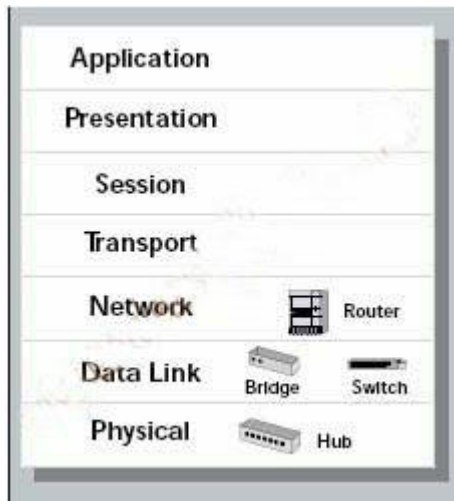
Every data link layer frame has two MAC addresses: a **source MAC address** of the host creating the frame and a **destination MAC address** for the device (or devices, in the cast of a broadcast or multicast) intended to receive the frame.

If only one device is to receive the frame, a unicast destination MAC address is used. If all devices need to receive the frame, a destination broadcast address is used.

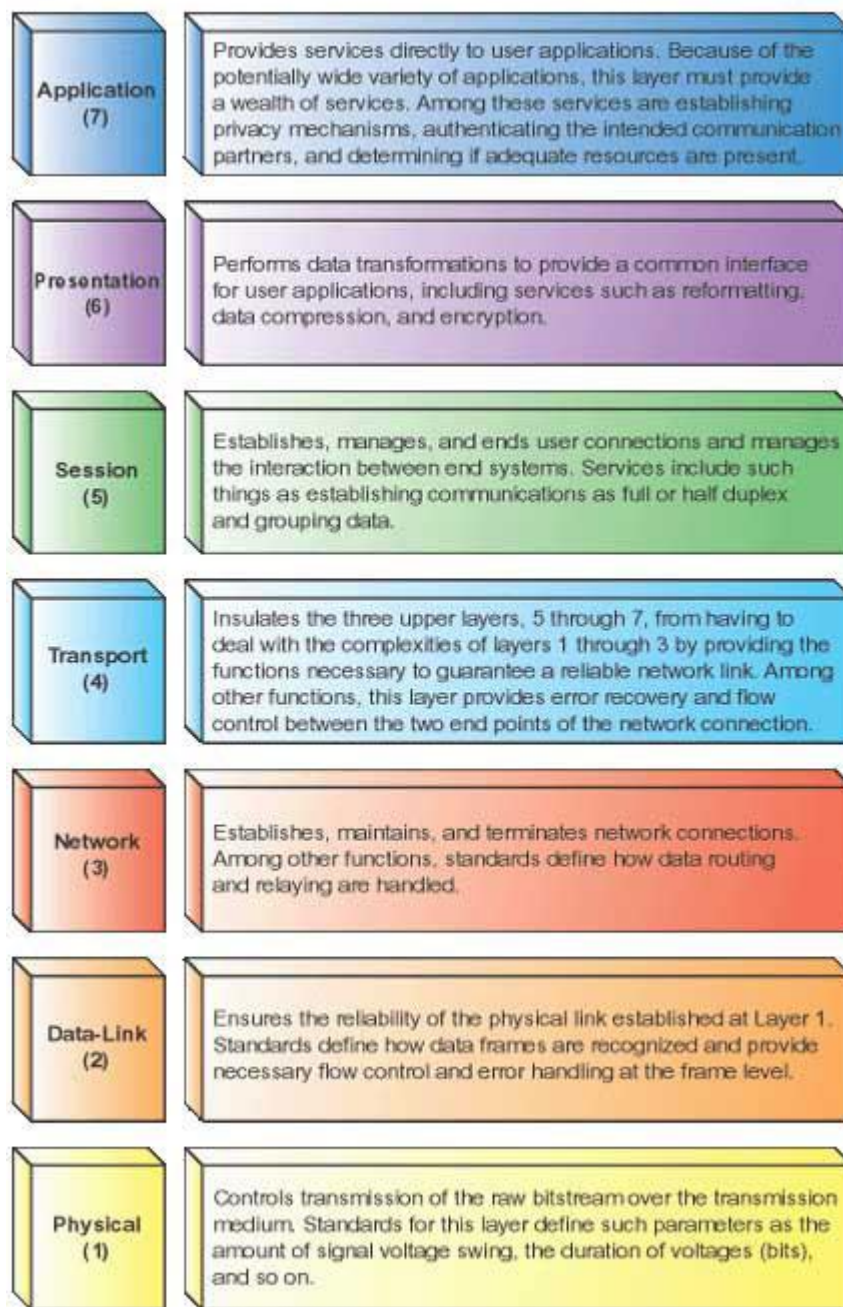
When all the binary bits are enabled for a MAC address, this is referred to as a **local broadcast address**: FFFF.FFFF.FFFF.

OSI (Open Systems Interconnect) layers and network components operate:

Hubs Switches, Bridges, Routers, NICs (Network Interface Card), WAPs (Wireless Access Point)



Seven layers of the OSI (Open Systems Interconnect) model and their functions.



Network protocols in terms of routing, addressing schemes, interoperability and naming conventions:

## TCP/IP

**Transmission Control Protocol**, A connection based Internet protocol responsible for breaking data into packets, which the IP protocol sends over the network. IP is located at the TCP/IP Internet layer which

corresponds to the network layer of the OSI Model. IP is responsible for routing packets by their IP address.

**IP** is a connectionless protocol. which means, IP does not establish a connection between source and destination before transmitting data, thus packet delivery is not guaranteed by IP. Instead, this must be provided by TCP. TCP is a connection based protocol and, is designed to guarantee delivery by monitoring the connection between source and destination before data is transmitted. TCP places packets in sequential order and requires acknowledgment from the receiving node that they arrived properly before any new data is sent.

### TCP/IP model

<b>Application layer</b>
DHCP - DNS - FTP - HTTP - IMAP4 - IRC - NNTP - XMPP - MIME - POP3 - SIP - SMTP - SNMP - SSH - TELNET - BGP - RPC - RTP - RTCP - TLS/SSL - SDP - SOAP - L2TP - PPTP
<b>Transport layer</b>
This layer deals with opening and maintaining connections, ensuring that packets are in fact received. This is where flow-control and connection protocols exist, such as: TCP - UDP - DCCP - SCTP - GTP
<b>Network layer</b>
IP (IPv4 - IPv6) - ARP - RARP - ICMP - IGMP - RSVP - IPSec - IPX/SPX
<b>Data link layer</b>
ATM - DTM - Ethernet - FDDI - Frame Relay - GPRS - PPP
<b>Physical layer</b>
Ethernet physical layer - ISDN - Modems - PLC - RS232 - SONET/SDH - G.709 - Wi-Fi

### IPX/SPX

IPX/SPX is the primary protocol of Novell NetWare (in particular, versions 4.0 and earlier, though it can be used on all versions). Internetwork Packet Exchange/Sequenced Packet Exchange developed by Novell and is used primarily on networks that use the Novell NetWare network

operating system. The IPX and SPX protocols provide services similar to those offered by IP and TCP. Like IP, IPX is a connectionless network layer protocol. SPX runs on top of IPX at the transport layer and, like TCP, provides connection oriented, guaranteed delivery. IPX/SPX provides many of the same features as TCP/IP, and is a routable transport protocol that allows networks to be segmented. However, network segmentation with IPX/SPX is done with network numbers and not with subnet masks. IPX/SPX is also similar to TCP/IP because IPX/SPX relies on internal protocols for network communication.

## IPX

IPX is similar to the operation of UDP of TCP/IP. IPX is a connectionless datagram transfer service. Because it is connectionless, like UDP, it does not require any preliminary connection setup to transmit the data packets. A disadvantage to connectionless communication is that flow control and error correction are not provided during network communication. In addition, packet delivery is not guaranteed. IPX also provides addressing and routing of packets within and between network segments.

## SPX

SPX is similar to the operation of TCP of TCP/IP. SPX is connection-oriented data transfer over IPX. Because SPX is connection oriented, flow control and error correction are provided along with packet delivery acknowledgments. SPX allows a single packet to remain unacknowledged at one time. If a packet is unacknowledged, the packet is retransmitted a total of 8 times. If there's no acknowledgment, SPX considers the connection failed.

## SPXII

SPXII is an enhancement to SPX. SPXII has several improvements over SPX. SPXII allows more than one packet to remain unacknowledged. SPXII also allows for a larger packet size, which improves network



performance by reducing the number of acknowledgment packets placed on the network.

## NetBEUI

NetBIOS Enhanced User Interface was designed as a small, efficient protocol for use in department-sized LANs of 20-200 computers that do not need to be routed to other subnets. NetBEUI is used almost exclusively on small, non-routed networks. A LAN-only (non-routable) protocol used in early Windows networks based on the NetBIOS API, NetBEUI is a Windows protocol that even Microsoft doesn't recommend for any but the most isolated networks. NetBEUI isn't required for NetBIOS functionality. As an extension of NetBIOS, NetBEUI is not routable, therefore networks supporting NetBEUI must be connected with bridges, rather than routers, like NetBIOS, the NetBEUI interface must be adapted to routable protocols like TCP/IP for communication over WANs.

## AppleTalk

The AppleTalk routing protocol is, amazing as it may sound, used by Macintosh networks. There are two important factors to understand about the AppleTalk protocol: zones and network numbers. AppleTalk network numbers assign AppleTalk networks unique numerical values that identify them as segments. Clients and servers can be part of only one network number. Because AppleTalk is routable, clients can access servers from any network number. AppleTalk also uses zones to aid clients in browsing an AppleTalk network. Zones allow servers, printers, and clients to be grouped logically for the purpose of resource access. Unlike network numbers, servers, printers, and clients can be part of more than one zone. Having membership in more than one zone allows clients easier access to network resources. Clients need not use the Chooser to view the resources of multiple zones.

## TCP (Transmission Control Protocol)

Transmission Control Protocol uses a reliable delivery system to deliver layer 4 segments to the destination. This would be analogous to using a certified, priority, or next-day service with the Indian Speed Post;Service. For example, with a certified letter, the receiver must sign for it, indicating the destination actually received the letter: proof of the delivery is provided. **TCP** operates under a similar premise: it can detect whether or not the destination received a sent segment. With the postal example, if the certified letter got lost, it would be up to you to resend it; with TCP, you don't have to worry about what was or wasn't received—TCP will take care of all the tracking and any necessary resending of lost data for you. TCP's main responsibility is to provide a reliable full-duplex, connection-oriented, logical service between two devices.

**TCP** goes through a three-way handshake to establish a session before data can be sent. Both the source and destination can simultaneously send data across the session. It uses windowing to implement flow control so that a source device doesn't overwhelm a destination with too many segments. It supports data recovery, where any missed or corrupted information can be re-sent by the source. Any packets that arrive out of order, because the segments traveled different paths to reach the destination, can easily be reordered, since segments use sequence numbers to keep track of the ordering.

## UDP (User Datagram Protocol)

**UDP** uses a best-effort delivery system, similar to how first class and lower postal services of the Indian Postal Service work. With a first class letter (post card), you place the destination address and put it in your mailbox, and hope that it arrives at the destination.

With this type of service, nothing guarantees that the letter will actually arrive at the destination, but in most instances, it does. If, however, the letter doesn't arrive at the destination, it's up to you, the letter writer, to resend the letter: the post office isn't going to perform this task for you.

UDP operates under the same premise: it does not guarantee the delivery of the transport layer segments. While TCP provides a reliable connection, UDP provides an unreliable connection.

**UDP** doesn't go through a three-way handshake to set up a connection—it simply begins sending the data. Likewise, UDP doesn't check to see whether sent segments were received by a destination; in other words, it doesn't use an acknowledgment

### Some commonly used ports

Port Number	Service
80	HTTP
21	FTP
110	POP3
25	SMTP
23	Telnet

### FTP (File Transfer Protocol)

One of the earliest uses of the Internet, long before Web browsing came along, was transferring files between computers. The **File Transfer Protocol (FTP)** is used to connect to remote computers, list shared files, and either upload or download files between local and remote computers. **FTP** runs over TCP, which provides a connection-oriented, guaranteed data-delivery service. **FTP** is a character-based command interface, although many FTP applications have graphical interfaces. **FTP** is still used for file transfer purposes, most commonly as a central FTP server with files available for download. Web browsers can make FTP requests to download programs from links selected on a Web page.

You should become familiar with the basic commands available in an FTP session. To begin a characterbased command session on a Windows computer, follow these steps.

- Open a Command prompt window, type **ftp** at the prompt, and press Enter.
- This will begin an FTP session on the local machine but will not initialize a connection to another machine.

- Without a connection to another machine, you will not be able to do anything. To connect, type ***open example.com*** or ***open 10.10.10.1***, in which *exmple.com* or *10.10.10.1* is the name or IP address of a host that is available as an FTP server. Most FTP servers require a logon id and password, or they will accept anonymous connections. At this point you will be prompted for a logon ID and password.
- Once you are connected, you can list the files on the remote server by typing ***dir***.
- If you have create privileges on the remote server, you can create a new directory by typing ***mkdir***.
- To download a file, type ***get filename.txt*** where *filename.txt* is the name of the file you are downloading. To upload a file, type ***put filename.txt***.

## SFTP (Secure File Transfer Protocol)

SSH File Transfer Protocol or SFTP is a network protocol that provides file transfer and manipulation functionality over any reliable data stream.

## TFTP (Trivial File Transfer Protocol)

TFTP is used when a file transfer does not require an acknowledgment packet during file transfer. TFTP is used often in router configuration. TFTP is similar in operation to FTP. TFTP is also a command-line-based utility.

One of the two primary differences between TFTP and FTP is ***speed*** and ***authentication***. Because TFTP is used without acknowledgment packets, it is usually faster than FTP. TFTP does not provide user authentication like FTP and therefore the user must be logged on to the client and the files on the remote computer must be writable. TFTP supports only unidirectional data transfer (unlike FTP, which supports bi-directional transfer). TFTP is operated over port 69.

## SMTP (Simple Mail Transfer Protocol)

SMTP is a standard electronic-mail protocol that handles the sending of mail from one SMTP to another SMTP server. To accomplish the transport, the SMTP server has its own MX (mail exchanger) record in the DNS

database that corresponds to the domain for which it is configured to receive mail.

When equipped for two-way communication, mail clients are configured with the address of a POP3 server to receive mail and the address of an SMTP server to send mail. The clients can configure server parameters in the properties sheets of the mail client, basing the choices on an FQDN or an IP address.

SMTP uses TCP for communication and operates on port 25. Simple Mail Transfer Protocol (SMTP) is the application-layer protocol used for transmitting e-mail messages. SMTP is capable of receiving e-mail messages, but it's limited in its capabilities. The most common implementations of SMTP are in conjunction with either POP3 or IMAP4. For example, users download an e-mail message from a POP3 server, and then transmit messages via an SMTP server

## HTTP (Hypertext Transfer Protocol)

HTTP is often called the protocol of the Internet. HTTP received this designation because most Internet traffic is based on HTTP. When a user requests a Web resource, it is requested using HTTP. The following is a Web request:

<http://www.example.com>

When a client enters this address into a Web browser, DNS is called to resolve the Fully Qualified Domain Name (FQDN) to an IP address. When the address is resolved, an HTTP get request is sent to the Web server. The Web server responds with an HTTP send response. Such communication is done several times throughout a single session to a Web site. HTTP uses TCP for communication between clients and servers. HTTP operates on port 80.

## HTTPS (Hypertext Transfer Protocol Secure)

HTTP is for Web sites using additional security features such as certificates. HTTPS is used when Web transactions are required to be secure. HTTPS uses a certificatebased technology such as VeriSign.

Certificate-based transactions offer a mutual authentication between the client and the server. Mutual authentication ensures the server of the client identity, and ensures the client of the server identity. HTTPS, in addition to using certificate-based authentication, encrypts all data packets sent during a session.

Because of the encryption, confidential user information cannot be compromised. To use HTTPS, a Web site must purchase a certificate from a third-party vendor such as VeriSign, CertCo, United States Postal Service, or other certificate providers. When the certificate is issued to a Web site from a third-party vendor, the Web site is using trusted communication with the client. The communication is trusted because the third party is not biased toward either the Web site or the client. To view a certificate during a HTTPS session, simply double-click the lock icon in the lower-right area of the Web browser. HTTPS operates on port 443 and uses TCP for communication.

### POP3 / IMAP4 (Post Office Protocol version 3 / Internet Message Access Protocol version 4)

Post Office Protocol 3 (POP3) and Internet Message Access Protocol 4 (IMAP4) are two application-layer protocols used for electronic messaging across the Internet. POP3 is a protocol that involves both a server and a client. A POP3 server receives an e-mail message and holds it for the user. A POP3 client application periodically checks the mailbox on the server to download mail. POP3 does not allow a client to send mail, only to receive it. POP3 transfers e-mail messages over TCP port 110.

IMAP4 is an alternate e-mail protocol. IMAP4 works in the same way as POP3, in that an e-mail message is held on a server and then downloaded to an e-mail client application. Users can read their e-mail message locally in their e-mail client application, but they can't send an e-mail message using IMAP4. When users access e-mail messages via IMAP4, they have the option to view just the message header, including its title and the sender's name, before downloading the body of the message. Users can create, change, or delete folders on the server, as well as search for messages and delete them from the server.

To perform these functions, users must have continued access to the IMAP server while they are working with e-mail messages. With IMAP4, an e-mail message is copied from the server to the e-mail client. When a user deletes a message in the e-mail client, the message remains on the server until it is deleted on the server. POP3 works differently in that an e-mail message is downloaded and not maintained on the server, unless configured otherwise. Therefore, the difference between POP3 and IMAP4 is that IMAP4 acts like a remote file server, while POP3 acts in a store-and-forward manner in its default configuration. (You can configure POP3 clients to leave copies of messages on the server, if you prefer.)

Both Microsoft and Netscape Web browsers have incorporated POP3. In addition, the Eudora and Microsoft Outlook Express e-mail client applications support both POP3 and IMAP4.

## Telnet

Short for Telecommunication Network, a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts on the network. Many people use remote control applications to access computers at their workplace from outside the network. In remote control, a session appears in which the user is able to manage the files on the remote computer, although the session appears to be functioning locally. Telnet is an early version of a remote control application.

Telnet is very basic; it offers solely character-based access to another computer. If you want to see a person's graphical desktop, you would need a different type of protocol, such as Remote Desktop Protocol (RDP), Independent Computing Architecture (ICA), or X Windows. Telnet acts as a user command with an underlying Transmission Control Protocol/Internet Protocol (TCP/IP) protocol that handles the establishment, maintenance, and termination of a remote session. The difference between using Telnet and a protocol such as File Transfer Protocol (FTP), is that Telnet logs you directly on to the remote host, and you see a window into that session on your local computer. A typical Telnet command might be as follows:

telnet example.com

Because this particular host is invalid, this command will have no result. However, if it were a valid host the remote computer would ask you to log on with a user ID and password. A correct ID and password would allow you to log on and execute Telnet commands.

You can often use Telnet to manage equipment that lacks a monitor. For example, most routers have Telnet enabled so that the administrator can log in and manage the router. Telnet also provides a quick check to make certain that network connectivity is functioning. Because Telnet sits at the application layer, if it can connect to a remote host, you can be certain that network connectivity between the two hosts is operational, as well as all lower-layer protocols.

## SSH (Secure Shell)

is a program for logging in to and executing commands on a remote machine. It provides secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel. When SSH connects and logs in to a specified computer, the user must prove his/her identity to the remote machine which is transmitted across the connection using one of three forms of data encryption. This process makes SSH impervious to Internet eavesdroppers who might otherwise steal account information.

## ICMP (Internet Control Message Protocol)

ICMP provides network diagnostic functions and error reporting. One of the most used IP commands is the Packet Internet Grouper (PING) command. When a host PINGS another client, it sends an ICMP ECHO request, and the receiving host responds with an ICMP ECHO REPLY. PING checks network connectivity on clients and routers. ICMP also provides a little network help for routers. When a router is being overloaded with route requests, the router sends a source quench message to all clients on the network, instructing them to slow their data requests to the router.



## ARP / RARP (Address Resolution Protocol / Reverse Address Resolution Protocol)

The Address Resolution Protocol (ARP) is an Internet layer protocol that helps TCP/IP network components find other devices in the same broadcast domain. ARP uses a local broadcast (255.255.255.255) at layer 3 and FF:FF:FF:FF:FF:FF at layer 2 to discover neighboring devices. Basically stated, you have the IP address you want to reach, but you need a physical (MAC) address to send the frame to the destination at layer 2. ARP resolves an IP address of a destination to the MAC address of the destination on the same data link layer medium, such as Ethernet. Remember that for two devices to talk to each other in Ethernet (as with most layer 2 technologies), the data link layer uses a physical address (MAC) to differentiate the machines on the segment. When Ethernet devices talk to each other at the data link layer, they need to know each other's MAC addresses.

RARP is sort of the reverse of an ARP. In an ARP, the device knows the layer 3 address, but not the data link layer address. With a RARP, the device doesn't have an IP address and wants to acquire one. The only address that this device has is a MAC address. Common protocols that use RARP are BOOTP and DHCP

## NTP (Network Time Protocol)

The Network Time Protocol is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. It provides accuracy's typically within a millisecond on LANs and up to a few tens of milliseconds on WANs.

## SNMP

SNMP is a two-way network management protocol. SNMP consists of two components, the SNMP Agent, and the SNMP Management Console. The SNMP Management Console is the server side for SNMP. The management

console sends requests to the SNMP Agents as get commands that call for information about the client.

The SNMP Agent responds to the Management Console's get request with a trap message. The trap message has the requested information for the Management Console to evaluate. Security can be provided in many ways with SNMP; however, the most common form of security for SNMP is the use of community names, associations that link SNMP Agents to their Management Consoles:

- Agents, by default, respond only to Management Consoles that are part of the same community name.
- If an SNMP Agent receives a request from a Management Console that is not part of the same community name, then the request for information is denied.

Because SNMP is an industry-standard protocol, heterogeneous environments are common. Many vendors provide versions of SNMP Management Consoles. Hewlett Packard, for example provides HP Open View (one of the most popular Management Consoles on the market); Microsoft provides SNMP Server with the Windows NT and 2000 Resource Kits and Systems Management Server. SNMP Management Consoles request information according to a Management Information Base (MIB) format. An MIB is a numeric value that specifies the type of request, and to which layer of the OSI model the request is being sent.

## SCP (Secure Copy Protocol)

Secure Copy or SCP is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. The protocol itself does not provide authentication and security; it expects the underlying protocol, SSH, to secure this.

The SCP protocol implements file transfers only. It does so by connecting to the host using SSH and there executes an SCP server (scp). The SCP server program is typically the very same program as the SCP client.

## LDAP (Lightweight Directory Access Protocol)

Lightweight Directory Access Protocol, or LDAP, is a networking protocol for querying and modifying directory services running over TCP/IP.

A directory is a set of information with similar attributes organized in a logical and hierarchical manner. The most common example is the telephone directory, which consists of a series of names organized alphabetically, with an address and phone number attached.

An LDAP directory often reflects various political, geographic, and/or organizational boundaries, depending on the model chosen. LDAP deployments today tend to use Domain Name System (DNS) names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organizational units, printers, documents, groups of people or anything else which represents a given tree entry.

## IGMP (Internet Group Multicast Protocol)

The Internet Group Management Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

## LPR (Line Printer Remote)

The Line Printer Daemon protocol/Line Printer Remote protocol (or LPD, LPR) also known as the Berkeley printing system, is a set of programs that provide printer spooling and network print server functionality for Unix-like systems.

The most common implementations of LPD are the official BSD UNIX operating system and the LPRng project. The Common Unix Printing System (or CUPS), which is more common on modern Linux distributions, borrows heavily from LPD.

A printer that supports LPD/LPR is sometimes referred to as a "TCP/IP printer" (TCP/IP is used to establish connections between printers and workstations on a network), although that term seems equally applicable to a printer that supports CUPS.

## **IP ADDRESS IPV4 IPV6 PUBLIC IP PRIVATE IP APIPA STATIC DYNAMIC IP CLASSES**

Systems that have interfaces to more than one network require a unique IP address for each network interface. The first part of an Internet address identifies the network on which the host resides, while the second part identifies the particular host on the given network. This creates the two-level addressing hierarchy.

The leading portion of each IP address identifies the network prefix. All hosts on a given network share the same network prefix but must have a unique host number. Similarly, any two hosts on different networks must have different network prefixes but may have the same host number.

An IP is a 32-bit number comprised of a host number and a network prefix, both of which are used to uniquely identify each node within a network. A shortage of available IP addresses has prompted the creation of an addressing scheme known as Classless Inter-Domain Routing (CIDR). Among other capabilities, CIDR allows one IP address to designate many unique IP addresses within a network. In addition, the current version of the IP address, IPv4, is being upgraded to IPv6. The latter uses a 128-bit address, allowing for 2<sup>128</sup> total IP addresses, as opposed to IPv4's 2<sup>32</sup>.

### Internet Protocol version 4

IPv4 addresses are 32 bits in length. To make these addresses more readable, they are broken up into 4 bytes, or octets, where any 2 bytes are separated by a period. This is commonly referred to as dotted decimal notation.

Here's a simple example of an IP address: **10.1.1.1**

An additional value, called a subnet mask, determines the boundary between the network and host components of an address. When comparing IP addresses to other protocols' addressing schemes, TCP/IP addressing seems the most complicated.

## Internet Protocol version 6 (IPv6)

Whereas IPv4 addresses use a dotted-decimal format, where each byte ranges from 0 to 255.

IPv6 addresses use eight sets of four hexadecimal addresses (16 bits in each set), separated by a colon (:),

like this: **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx** (x would be a hexadecimal value).

This notation is commonly called string notation.

- Hexadecimal values can be displayed in either lower- or upper-case for the numbers **A–F**.
- A leading zero in a set of numbers can be omitted; for example, you could either enter **0012** or **12** in one of the eight fields—both are correct.
- If you have successive fields of zeroes in an IPv6 address, you can represent them as two colons (::). For example, **0:0:0:0:0:0:0:5** could be represented as **::5**; and **ABC:567:0:0:8888:9999:1111:0** could be represented as **ABC:567::8888:9999:1111:0**. However, you can only do this once in the address: **ABC::567::891::00** would be invalid since :: appears more than once in the address. The reason for this limitation is that if you had two or more repetitions, you wouldn't know how many sets of zeroes were being omitted from each part.
- An unspecified address is represented as ::, since it contains all zeroes.

## Classful IP (Internet Protocol) Ranges and Their Subnet Masks

When dealing with IP addresses, the address is broken into two components:

**Network component** Defines on what segment, in the network, a device is located

**Host component** Defines the specific device on a particular network segment

The network number uniquely identifies a segment in the network and a host number uniquely identifies a device on a segment. The combination of these two numbers must be unique throughout the entire network. TCP/IP uses the same two components for addressing, but it adds a twist by breaking up network numbers into five classes: A, B, C, D, and E. Each of these classes has a predefined network and host boundary:

- **Class A address**,The first byte is a network number (8 bits) and the last 3 bytes are for host numbers (24 bits).
- **Class B address** ,The first 2 bytes are a network number (16 bits) and the last 2 bytes are for host numbers (16 bits).
- **Class C address** ,The first 3 bytes are a network number (24 bits) and the last 1 byte is for host numbers (8 bits).
- **Class D and E** ,addresses Class D Used for multicasting and Class E addresses are reserved.

What distinguishes the different classes of addresses are the settings to which the first bit to 5 bits are set:

- Class **A** addresses always begin with a **0** in the highest order bit.
- Class **B** addresses always begin with **10** in the highest order bits.
- Class **C** addresses always begin with **110** in the highest order bits.
- Class **D** addresses always begin with **1110** in the highest order bits.
- Class **E** addresses always begin with **11110** in the highest order bits.

When talking about the highest order bit or bits, this includes all 32 bits. Therefore, this would be the very first bit on the left of the address (the most significant bit). If the first octet contains 1000001, this represents 129 in decimal, which would be a Class B address. Given these

distinctions with the assigned high order bit values, it is easy to predict, for a given address, to what class of network numbers it belongs:

Class A addresses range from	1-126:	00000001-01111111
Class B addresses range from	128-191:	10000000-10111111
Class C addresses range from	192-223:	11000000-11011111
Class D addresses range from	224-239:	11100000-11101111
Class E addresses range from	240-254:	

0 is reserved and represents all IP addresses;  
127 is a reserved address and is used for loop back testing;  
255 is a reserved address and is used for broadcasting  
purposes.

Given these restrictions with beginning bit values, it is fairly easy to predict what address belongs to what class. Simply look at the first number in the dotted-decimal notation and see which range it falls into.

When you are dealing with IP addresses, two numbers are always reserved for each network number:

**The first address in the network represents the network's address, and the last address in the network represents the broadcast address for this network, called *directed broadcast*.**

When you look at IP itself, two IP addresses are reserved: 0.0.0.0 (the very first address), which represents all IP addresses, and 255.255.255.255 (the very last address), which is the local broadcast address.

### Purpose of subnetting.

Subnetting allows you to break up and use an addressing space more efficiently. Basically, subnetting steals the higher-order bit or bits from the host component and uses these bits to create more subnets with a smaller number of host addresses in each of these subnets.

Subnet masks are 32 bits long and are typically represented in dotted-decimal (such as 255.255.255.0) or the number of networking bits (such as /24). The networking bits in a mask must be contiguous and the host bits in the subnet mask must be contiguous. 255.0.255.0 is an invalid mask. A subnet mask is used to mask a portion of the IP address, so that

TCP/IP can tell the difference between the network ID and the host ID. TCP/IP uses the subnet mask to determine whether the destination is on a local or remote network.

**Advantages of subnetting a network include the following:**

- Reducing network collision by limiting the range of broadcasts using routers
- Enabling different networking architectures to be joined

**Differences between private and public network addressing schemes.**

As to assigning addresses to devices, two general types of addresses can be used: public and private.

**Public addresses**

Public addresses are Class A, B, and C addresses that can be used to access devices in other public networks, such as the Internet. The Internet Assigned Numbers Authority (IANA) is ultimately responsible for handing out and managing public addresses. Normally you get public addresses directly from your ISP, which, in turn, requests them from one of five upstream address registries:

- American Registry for Internet Numbers (ARIN)
- Reseaux IP Europeans Network Coordination Center (RIPE NCC)
- Asia Pacific Registry for Internet Numbers (APNIC)
- Latin American and Caribbean Internet Address Registry (LACNIC)
- African Network Information Centre (AfriNIC)

**Private Addresses**

Within the range of addresses for Class A, B, and C addresses are some reserved addresses, commonly called private addresses. Anyone can use private addresses; however, this creates a problem if you want to access the Internet. Remember that each device in the network (in this case, this includes the Internet) must have a unique IP address. If two networks are using the same private addresses, you would run into reachability issues.



To access the Internet, your source IP addresses must have a unique Internet public address. This can be accomplished through address translation. Here is a list of private addresses that are assigned in RFC 1918:

- Class A: 10.0.0.0–10.255.255.255 (1 Class A network)
- Class B: 172.16.0.0–172.31.255.255 (16 Class B networks)
- Class C: 192.168.0.0–192.168.255.255 (256 Class C networks)

## IP (Internet Protocol) addressing methods:

### Static /Dynamic

Each device in an IP network is either assigned a permanent address (**static**) by the network administrator or is assigned a temporary address (**dynamic**) via DHCP software. Routers, firewalls and proxy servers use static addresses as do most servers and printers that serve multiple users. Client machines may use static or dynamic IP addresses. The IP address assigned to your service by your cable or DSL Internet provider is typically dynamic IP. In routers and operating systems, the default configuration for clients is dynamic IP.

### DHCP

DHCP stands for Dynamic Host Configuration Protocol. This protocol assigns network IP addresses to clients on the network at startup. With DHCP, each client workstation does not need to be set up with a static IP address. DHCP is recommended on large networks. It would be very time consuming to manually assign a static IP address to every workstation on your network.

With static IP addressing, the IP address that you assign to a device never changes. A DHCP server contains a pool of IP addresses that it can draw from to assign to devices that are connecting to the network. Other TCP/IP properties, such as default gateways, DNS servers, and subnet masks can also be assigned automatically.

## Self-assigned (APIPA (Automatic Private Internet Protocol Addressing))

Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems (included in Windows 98, ME, 2000, and XP) that enables a computer to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function.

Using APIPA, a Windows based client assigns itself an IP address from a range reserved for authorized private class B network addresses (**169.254.0.1 through 169.254.255.254**), with a subnet mask of **255.255.0.0**. A computer with an authorized private address cannot directly communicate with hosts outside its subnet, including Internet hosts.

APIPA is most suitable for small, single-subnet networks, such as a home or small office. APIPA is enabled by default if no DHCP servers are available on the network.

**Note** APIPA assigns only an IP address and subnet mask; it does not assign a default gateway, nor does it assign the IP addresses of DNS or WINS servers. Use APIPA only on a single-subnet network that contains no routers. If your small office or home office network is connected to the Internet or a private intranet, do not use APIPA.

## **NETWORK SECURITY PROTOCOLS CHAP MS-CHAP PAP RADIUS RAS PPP SLIP PPPOE PPTP RDP**

Security protocols protect a computer from attacks. To understand how security protocols work, you must first understand what types of attacks they protect against. Networks and data are vulnerable to both active attacks, in which information is altered or destroyed, and passive attacks, in which information is monitored. Attacks that you might encounter include the following:

### Altering data

This active attack takes place when data is interrupted in transit and modified before it reaches its destination, or when stored data is altered.

This passive attack takes advantage of network traffic that is transmitted across the wire in clear text. The attacker simply uses a device that monitors traffic and "listens in" to discover information. You'll hear this term referred to as **sniffing the wire**, and sometimes as **snooping**.

### IP address spoofing

One way to authenticate data is to check the IP address in data packets. If the IP address is valid, that data is allowed to pass into the private network. **IP address spoofing** is the process of changing the IP address so that data packets will be accepted. IP address spoofing can be used to modify or delete data, or to perpetuate an additional type of attack.

### Password pilfering

A hacker will obtain user IDs and passwords, or even encryption keys, to gain access to network data, which can then be altered, deleted, or even used to create another attack. This type of attack is usually done by asking unsuspecting users, reading sticky notes containing passwords that are posted next to computers, or sniffing the wire for password information. Sometimes a hacker will attempt to get hired at a company merely to obtain an ID and password with access rights to the network.

### Denial of service

This active attack is intended to cause full or partial network outages so that people will not be able to use network resources and productivity will be affected. The attacker floods so many packets through the network or through specific resources that other users can't access those resources. The denial-of-service attack can also serve as a diversion while the hacker alters information or damages systems.

### Virus

A virus is an attack on a system. It is a piece of software code that is buried inside a trusted application (or even an e-mail message) that invokes some action to wreak havoc on the computer or other network resources.

Security Method	Type of Attack	Notes
<b>Authentication</b>	Password guessing attacks	Verifies the user's identity
<b>Access control</b>	Password pilfering	Protects sensitive data from access by the average user
<b>Encryption</b>	Data alteration	Prevents the content of the packets from being tampered with
<b>Certificates</b>	Eavesdropping	Transmits identity information securely
<b>Firewalls</b>	Denial of service (as well as others)	When configured correctly, can prevent many denial-of-service attacks
<b>Signatures</b>	Data alteration	Protects stored data from tampering
<b>Public key infrastructure</b>	Spoofing	Ensures that data received is from correct sender
<b>Code authentication</b>	Virus and other code attacks	Protects the computer from altered executables
<b>Physical security</b>	Password pilfering	Protects unauthorized persons from having access to authorized users and their IDs and passwords
<b>Password policies</b>	Password pilfering	Ensures that passwords are difficult to guess or otherwise decipher

## IPSec (Internet Protocol Security)

IPSec Is a set of protocols used to support secure exchange of packets at the IP layer. IPsec supports two encryption modes: Transport and Tunnel.

**Transport mode** encrypts only the data portion of each packet, but leaves the header untouched.

**The more secure Tunnel mode** encrypts both the header and the data portion.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as **Internet Security Association and Key Management Protocol/Oakley**, which allows the receiver to obtain a public key and authenticate the sender using digital certificates. IPsec protocols operate at the network layer, layer 3 of the OSI model. Other Internet security protocols in widespread use, such as

SSL and TLS, operate from the transport layer up (OSI layers 4 - 7). This makes IPsec more flexible, as it can be used for protecting both TCP and UDP based protocols

### L2TP (Layer 2 Tunneling Protocol)

**Layer 2 Tunneling Protocol** is a tunneling protocol used to support virtual private networks VPNs. L2TP is an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks. L2TP combines the best features of two other tunneling protocols: **PPTP from Microsoft and L2F from Cisco Systems.**

### SSL (Secure Sockets Layer)

**Secure Sockets Layer** is a protocol that supplies secure data communication through data encryption and decryption. SSL enables communications privacy over networks by using a combination of public key, and bulk data encryption.

### WEP (Wired Equivalent Privacy)

**Wired Equivalent Privacy** is a scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks. Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network and thus it does not protect users of the network from each other.

### WPA (Wi-Fi Protected Access)

A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.

### WPA2 (Wi-Fi Protected Access 2)

WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

## 802.11x

IEEE 802.11 also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802). The term 802.11x is also used to denote this set of standards and is not to be mistaken for any one of its elements. There is no single 802.11x standard.

Protocol	Release Date	Op. Frequency	Data Rate (Typ)	Data Rate (Max)	Range (Indoor)	Range (Outdoor)
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	~25 meters	~75 meters
802.11b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	~35 meters	~100 meters
802.11g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	~25 meters	~75 meters
802.11n	2007	2.4 GHz or 5 GHz bands	200 Mbit/s	540 Mbit/s	~50 meters	~125 meters

## Identify authentication protocols:

### CHAP (Challenge Handshake Authentication Protocol)

Challenge Handshake Authentication Protocol is a challenge-response authentication protocol that uses the industry-standard Message Digest 5 (MD5) hashing scheme to encrypt the response. CHAP is used by various vendors of network access servers and clients.

### MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)

MS-CHAP Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is a nonreversible, encrypted password authentication protocol. The challenge handshake process works as follows:

- The remote access server or the IAS server sends a challenge to the remote access client that consists of a session identifier and an arbitrary challenge string.
- The remote access client sends a response that contains the user name and a nonreversible encryption of the challenge string, the session identifier, and the password.
- The authenticator checks the response and, if valid, the user's credentials are authenticated.

### PAP (Password Authentication Protocol)

Password Authentication Protocol uses plaintext passwords and is the least sophisticated authentication protocol. It is typically negotiated if the remote access client and remote access server cannot negotiate a more secure form of validation.

### RADIUS (Remote Authentication Dial-In User Service)

Is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations.

Some ISPs (commonly modem, DSL, or wireless 802.11 services) require you to enter a username and password in order to connect on to the Internet. Before access to the network is granted, this information is passed to a Network Access Server (NAS) device over the Point-to-Point Protocol (PPP), then to a RADIUS server over the RADIUS protocol. The RADIUS server checks that the information is correct using authentication schemes like PAP, CHAP or EAP.

If accepted, the server will then authorize access to the ISP system and select an IP address. RADIUS is also widely used by VoIP service providers.

Kerberos and EAP (Extensible Authentication Protocol)).

An authentication system, **Kerberos** is designed to enable two parties to exchange private information across an open network. It works by assigning a unique key, called a ticket, to each user that logs on to the network. The ticket is then embedded in messages to identify the sender of the message.

**Extensible Authentication Protocol**, or EAP, is a universal authentication framework frequently used in wireless networks and Point-to-Point connections. Although the EAP protocol is not limited to wireless LANs and can be used for wired LAN authentication, it is most often used in wireless LANs. Recently, the WPA and WPA2 standard has officially adopted five EAP types as its official authentication mechanisms.

### Smart Cards

Smart cards are gaining in popularity as a way to ensure secure authentication using a physical key. Smart cards are able to provide an interactive logon, secure e-mail messages, and authenticate access to network services.

Smart cards contain chips to store a user's private key and can also store logon information; public key certificates; and other information, depending on the smart card's usage. When a user needs to access a resource, the user inserts the smart card into a reader attached to the network. After typing in the user's personal identification number (PIN), the user is authenticated and can access network resources. The private key is automatically available for transparent access to encrypted information.

Smart cards require Public Key Infrastructure (PKI), a method of distributing encryption keys and certificates. In addition, each protected resource will require a smart-card reader. Some implementations of smart cards combine the smart card with employee badges so that employees need a single card for building and network access.

### Remote access protocols and services:

#### RAS (Remote Access Service)



Remote Access Service A service that provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users with RAS can dial in to remotely access their networks for services such as file and printer sharing, electronic mail, scheduling, and SQL database access.

## PPP (Point-to-Point Protocol)

PPP is based on an open standard defined in RFCs 1332, 1661, and 2153. PPP works with asynchronous and synchronous serial connections as well as High-Speed Serial Interfaces (HSSI) and ISDN interfaces (BRI and PRI).

### ***PPP***

### ***Components***

PPP has many more features than HDLC. Like HDLC, PPP defines a frame type and how two PPP devices communicate with each other, including the multiplexing of network and data link layer protocols across the same link. However, PPP also does the following:

- Performs dynamic configuration of links
- Allows for authentication
- Compresses packet headers
- Tests the quality of links
- Performs error detection and correction
- Allows multiple PPP physical connections to be bound together as a single logical connection (referred to as multilink)

### ***PPP has three main components:***

- Frame format (encapsulation)
- Link Control Protocol (LCP)
- Network Control Protocol (NCP)

Each of these three components plays an important role in the setup, configuration, and transfer of information across a PPP connection.

## SLIP (Serial Line Internet Protocol)

An older industry standard that is part of Windows remote access client to ensure interoperability with other remote access software.

### PPPoE (Point-to-Point Protocol over Ethernet)

Point-to-Point Protocol over Ethernet encapsulates PPP frames in Ethernet frames and is usually used in conjunction with ADSL services.

It gives you a lot of the familiar PPP features like authentication, encryption, and compression, but there's a downside—it has a lower maximum transmission unit (MTU) than standard Ethernet does, and if your firewall isn't solidly configured, this little attribute can really give you some grief! Still somewhat popular in the United States, PPPoE on Ethernet's.

main feature is that it adds a direct connection to Ethernet interfaces while providing DSL support as well. It's often used by many hosts on a shared Ethernet interface for opening PPP sessions to various destinations via at least one bridging modem.

### PPTP (Point-to-Point Tunneling Protocol)

Networking technology that supports multiprotocol virtual private networks (VPNs), enabling remote users to access corporate networks securely across the Internet or other networks by dialing into an Internet service provider (ISP) or by connecting directly to the Internet. The Point-to-Point Tunneling Protocol (PPTP) tunnels, or encapsulates, IP, IPX, or NetBEUI traffic inside of IP packets. This means that users can remotely run applications that are dependent upon particular network protocols.

### VPN (Virtual Private Network)

Virtual private network A remote LAN that can be accessed through the Internet by using PPTP (see above)

### RDP (Remote Desktop Protocol)

Remote Desktop Protocol (RDP) is a multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services. Clients exist for most versions of Windows (including handheld versions),

and other operating systems such as Linux, FreeBSD, Solaris Operating System and Mac OS X. The server listens by default on TCP port 3389.

- Version 4.0 was introduced with Terminal Services in Windows NT 4.0 Server, Terminal Server Edition.
- Version 5.0, introduced with Windows 2000 Server, added support for a number of features, including printing to local printers, and aimed to improve network bandwidth usage.
- Version 5.1, introduced with Windows XP Professional, included support for 24-bit color and sound.
- Version 5.2, introduced with Windows Server 2003, included support for console mode connections, a session directory, and local resource mapping.
- Version, 6.0, introduced with Windows Vista and Windows Server includes a significant number of new features, most notably being able to remotely access a single application instead of the entire desktop, and support for 32 bit color.

## **STAR TOPOLOGY RING TOPOLOGY BUS TOPOLOGY LOGICAL PHYSICAL MESH TOPOLOGY**

### Topologies

The first thing to consider about a network is its physical shape, or the design layout, which will be extremely important when you select a wiring scheme and design the wiring for a new installation.

Network really has two shapes, or two types of topology; one is physical and the other is logical. The physical topology is the shape you can see, and the logical topology is the shape that the data travels in.

### Physical Topologies

Physical topology is further divided in two section

- Point-to-point connections
- Multipoint connections

### Point-to-point connections

Only two devices are involved in a point-to-point connection, with one wire (or air, in the case of wireless) sitting between them. A point-to-point link is typified by two devices monopolizing the media-similar to two teenagers talking on the telephone with one another, not allowing anyone else to use the phone on either side.

### Multipoint connections

In a multipoint connection, multiple machines share the cabling. Multipoint connections might be a group of computers strung together in a long line on an old-fashioned ThinNet (10Base2) cable, or it could be a party line of telephones, all sharing a common phone connection. In fact, even your local cable TV provider uses a multipoint system to get every person in the neighborhood hooked up. In every multipoint connection, each device must be able to identify itself. This is where addressing at the hardware level starts. The device's address must be unique on the channel that it shares with those other devices, or else confusion reigns. Just ask any network administrator who has accidentally assigned the same logical address to two computers. It's not fun dealing with any type of addressing conflict.

### logical topology

A logical topology describes how components communicate across the physical topology. The physical and logical topologies are independent of each other. For example, any variety of Ethernet uses a logical bus topology when components communicate, regardless of the physical layout of the cabling. This means that in Ethernet, you might be using 10BaseT with a physical star topology to connect components together; however, these components are using a logical bus topology to communicate.

Media Type	Physical Topology	Logical Topology
Ethernet	Bus, star, or point-to-point	Bus
FDDI	Ring	Ring

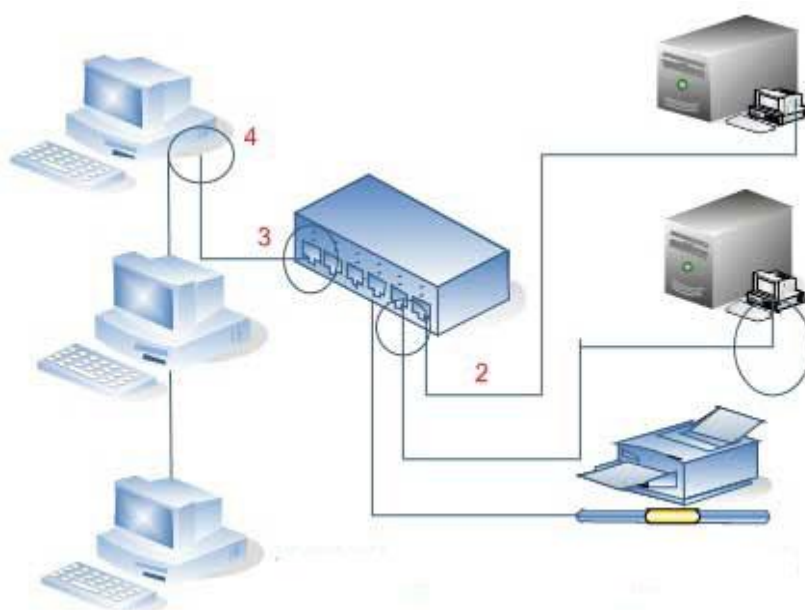
Token Ring	Star	Ring
------------	------	------

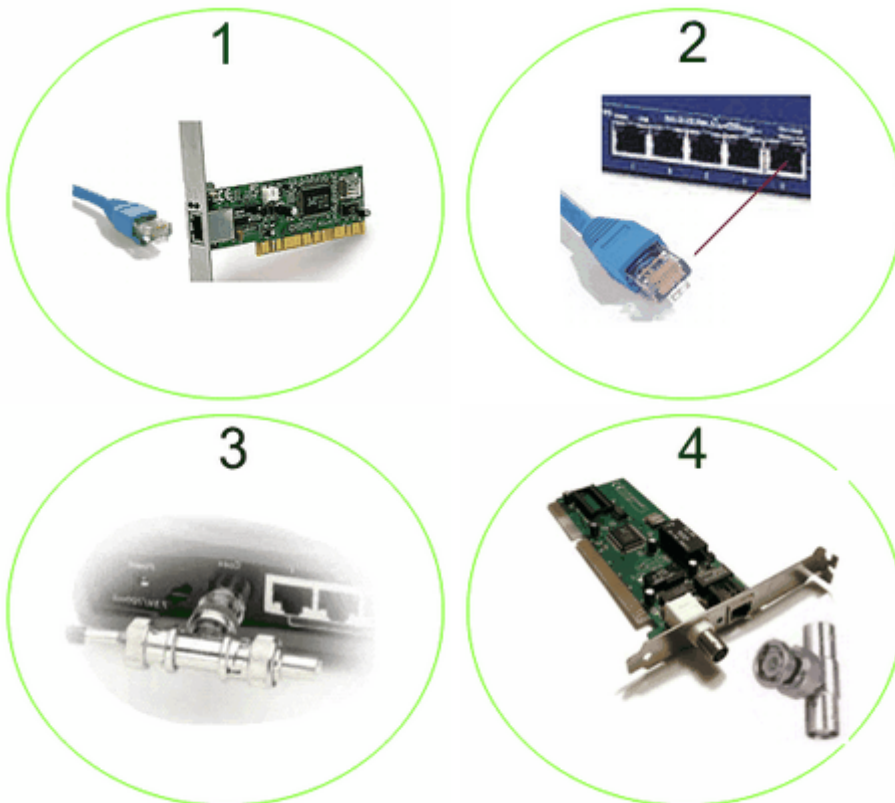
Token Ring is another good example of a communication protocol that has a different physical topology from its logical one. Physically, Token Ring uses a star topology, similar to 10BaseT Ethernet. Logically, however, Token Ring components use a ring topology to communicate between devices. This can create confusion when you are trying to determine how components are connected together and how they communicate. FDDI, on the other hand, is straightforward. FDDI's physical and logical topologies are the same: a ring.

## Ethernet Networks

In late 1978, the first experimental network system was created to interconnect the **Xerox Altos** PCs to one another and to servers and laser printers. This first experimental network was called the ***Alto Aloha Network***.

In 1979 the name was changed to ***Ethernet***, to make it clear that the system could support any computer not just Altos and to point out that the new network mechanisms had evolved well beyond the Aloha system. The **base** word ether was chosen as a way of describing an essential feature of the system; the physical medium (a cable) carries bits to all stations





In the diagram you can see two ethernet configurations. On the left the computers are connected together with a single cable coming from the router/switch, this is called a bus or thin ethernet configuration. On the right side of the diagram each computer connects directly to the router/switch. this is how most ethernets are configured today. In this topology management of the network is made much easier (such as adding and removing devices), because of the central point. If computers are connected in a row, along a single cable this is called a bus topology, if they branch out from a single junction or hub this is known as a star topology. When computers are connected to a cable that forms a continuous loop this is called a ring topology. We will go through all of these topologies in coming section.

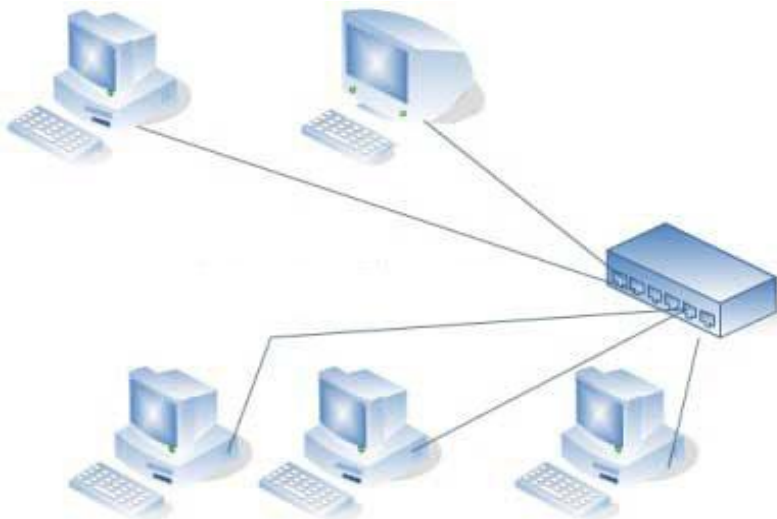
### Star Topology

A star configuration is simple: Each of several devices has its own cable that connects to a central hub, or sometimes a switch, multipoint repeater, or even a Multistation Access Unit (MAU). Data passes through the hub to reach other devices on the network. Ethernet over unshielded

twisted pair (UTP), whether it is 10BaseT, 100BaseT, or Gigabit, all use a star topology.

Star networks are one of the most common computer network topologies. In its simplest form, a star network consists of one central switch, hub or computer which acts as a router to transmit messages. If the central node is passive, the originating node must be able to tolerate the reception of an echo of its own transmission, delayed by the two-way transmission time (i.e. to and from the central node) plus any delay generated in the central node. An active star network has an active central node that usually has the means to prevent echo-related problems.

The star topology reduces the chance of network failure by connecting all of the systems to a central node. When applied to a bus-based network, this central hub rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, sometimes including the originating node. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. The failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the rest of the systems will be unaffected.



You will find that a star topology is most common in networks. This is mainly because of the ease of configuring and troubleshooting it. If a wire or a single port on the hub or switch goes bad, only one network node goes down, which prevents a huge impact on productivity overall (unless the entire hub or switch fails-in which case, the whole LAN goes down).

However, because a star topology involves a central hub or switch as well as a lot more cabling, it costs more to implement.

### **Disadvantages of a Star Network**

- Twisted pair cables typically used in star topologies are not as immune to interferences as coaxial cable
- Expensive because of additional cabling and central hub require
- If the centralize device fails the entire system is affected.

### **Advantages of Star Network**

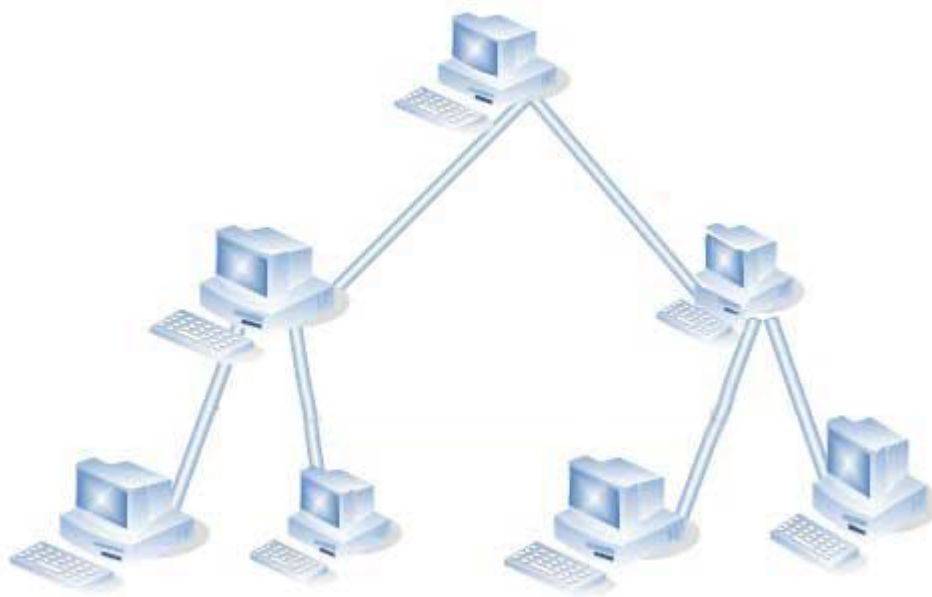
- Easy to Install: Each device on network simply requires a cable run between it and the concentrator device.
- Flexible: Devices can be added or removed without affecting the other devices on the network.
- A single device or cable failure will not bring down the network
- Easy to set up and to expand.as each device on the network simply requires a cable run between it and the concentrator device
- Any non-centralised failure will have very little effect on the network, whereas on a ring network it would all fail with one fault.
- Data Packets are sent quickly as they do not have to travel through any unnecessary nodes.
- Performance is greater with speeds capable of 10mbps to 100mbps or more
- The ability to isolate individual devices in troubleshooting An intelligent central hub or switch that can help diagnose and manage the network  
Adjusting traffic levels so that computers that place heavy loads on the network are moved to separate hubs

### **Hierarchical Topology (also known as Tree)**

The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes



that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link, the top level central 'root' node being the only node that has no other node above it in the hierarchy - the hierarchy of the tree is symmetrical, each node in the network having a specific fixed number,  $f$ , of nodes connected to it at the next lower level in the hierarchy, the number,  $f$ , being referred to as the 'branching factor' of the hierarchical tree.



### **Notes:**

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

- The total number of point-to-point links in a network that is based upon the physical hierarchical topology will be one less than the total number of nodes in the network.
- If the nodes in a network that is based upon the physical hierarchical topology are required to perform any processing upon the data that is transmitted between nodes in the network, the nodes that are at higher levels in the hierarchy will be required to perform more processing operations on behalf of other nodes than the nodes that are lower in the hierarchy.

## Bus Topology

In bus topologies, all computers are connected to a single cable or "trunk or backbone", by a transceiver either directly or by using a short drop cable. All ends of the cable must be terminated, that is plugged into a device such as a computer or terminator. Most bus topologies use coax cables.



The number of computers on a bus network will affect network performance, since only one computer at a time can send data, the more computers you have on the network the more computers there will be waiting send data. A line break at any point along the trunk cable will result in total network failure. Computers on a bus only listen for data being sent they do not move data from one computer to the next, this is called passive topology.

### **Disadvantages**

- Entire network shuts down if there is a break in the main cable.
- Difficult to identify the problem if the entire network shuts down.
- Performance: Coax technology is usually limited to a maximum of 10mbps.
- Not intended for use as a standalone solution in a large building.
- Coax technology is usually limited to a maximum of 10mbps.
- Limited cable length and number of stations.

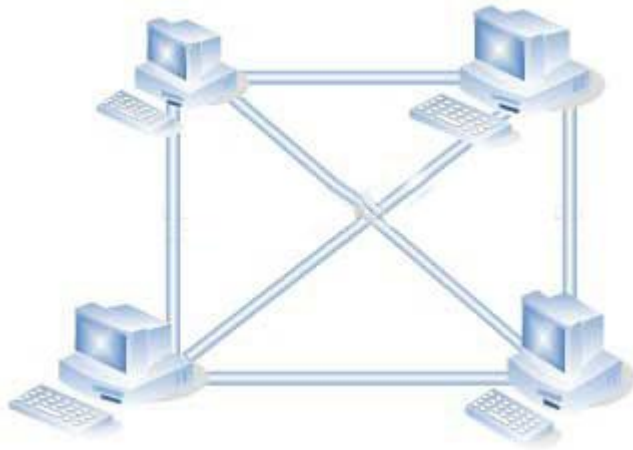
- Not intended for use as a standalone solution in a large building.
- If there is a problem with the cable, the entire network goes down.
- Performance degrades as additional computers are added or on heavy traffic.
- Low security (all computers on the bus can see all data transmissions).
- If one node fails, the whole network will shut down.
- You are limited with the number of devices that you can have on a single segment.

### **Advantages**

- Inexpensive: Does not require additional hardware to interconnect the attached devices.
- Easy to Install: Coax cable is durable and performs well in harsh environments.
- Flexible: New devices can be added by simply installing a new 'T' connector.
- Well suited for temporary or small networks not requiring high speeds(quick setup)
- Initially less expensive than other topologies.
- Requires less cable length than a star topology

### **MeshTopology**

A Mesh topology Provides each device with a point-to-point connection to every other device in the network. These are most commonly used in WAN's, which connect networks over telecommunication links. Mesh topologies use routers to determine the best path. Mesh networks provide redundancy, in the event of a link failure, meshed networks enable data to be routed through any other site connected to the network. Because each device has a point-to-point connection to every other device, mesh topologies are the most expensive and difficult to maintain.



Mesh networks differ from other networks in that the component parts can all connect to each other via multiple hops, and they generally are not mobile. Mobile ad-hoc networking (MANET), featured in many consumer devices, is a subsection of mesh networking. Mesh networks are self-healing: the network can still operate even when a node breaks down or a connection goes bad. As a result, a very reliable network is formed.

This concept is applicable to wireless networks, wired networks, and software interaction. There are three distinct generations of wireless mesh architectures. In the first generation one radio provides both backhaul (packet relaying) and client services (access to a laptop). In the second generation, one radio relayed packets over multiple hops while another provided client access. This significantly improved backhaul bandwidth and latency. Third generation wireless mesh products use two or more radios for the backhaul for higher bandwidth and low latency. Third generation mesh products are replacing previous generation products as more demanding applications like voice and video need to be relayed wirelessly over many hops of the mesh network.

### **Advantages of Mesh topology**

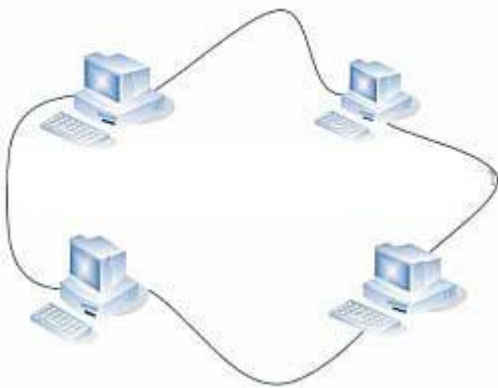
- Extremely reliable. Data has access to fastest paths and can load balance.
- Provides redundancy and fault tolerance between devices and ensures the best possibility that the network is always available.

### **Diadvantage of Mesh**

- Uses the most cabling to implement.
- Has a high administrative overhead.

## Ring

In a ring topology network computers are connected by a single loop of cable, the data signals travel around the loop in one direction, passing through each computer. Ring topology is an active topology because each computer repeats (boosts) the signal before passing it on to the next computer. One method of transmitting data around a ring is called token passing. The token is passed from computer to computer until it gets to a computer that has data to send.



If there is a line break, or if you are adding or removing a device anywhere in the ring this will bring down the network. In an effort to provide a solution to this problem, some network implementations (such as FDDI) support the use of a double-ring. If the primary ring breaks, or a device fails, the secondary ring can be used as a backup.

### **Advantages**

- Data is quickly transferred without a 'bottle neck'
- The transmission of data is relatively simple as packets travel in one direction only.
- Adding additional nodes has very little impact on bandwidth
- It prevents network collisions because of the media access method or architecture required.
- All devices have equal access.

### **Disadvantages**

- Because all stations are wired together, to add a station you must shut down the network temporarily.
- It is difficult to troubleshoot the ring.
- Data packets must pass through every computer between the sender and recipient Therefore this makes it slower.
- If any of the nodes fail then the ring is broken and data cannot be transmitted successfully.

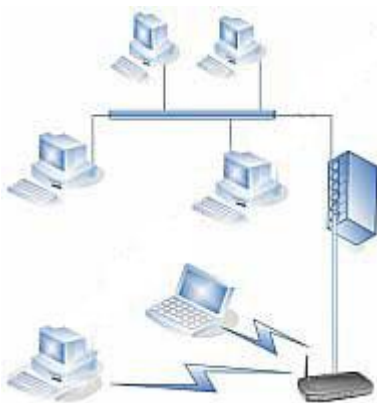
## Wireless

A wireless network consists of wireless NICs and access points. NICs come in different models including PC Card, ISA, PCI, etc. Access points act as wireless hubs to link multiple wireless NICs into a single subnet. Access points also have at least one fixed Ethernet port to allow the wireless network to be bridged to a traditional wired Ethernet network, such as the organization's network infrastructure. Wireless and wired devices can coexist on the same network.

Wireless topologies seem odd at first because there are no physical wires to guide you to the actual topology shapes that they use. In fact, wireless topologies are implemented in a star, a mesh, or a cellular configuration.

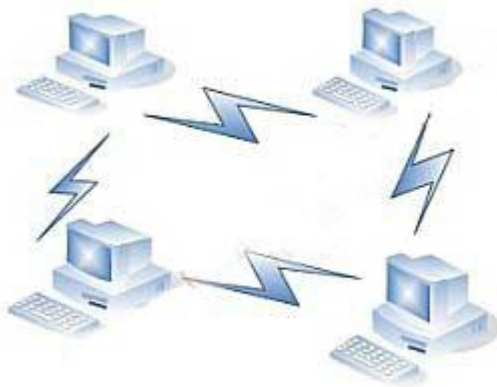
## BSS wireless topology

In the star configuration, the wireless topology is called a Basic Service Set (BSS). It consists of a wireless access point connected to a wired network, and it enables each wireless device to connect to the access point and through it to all other devices.



## Independent Basic Service Set (IBSS)

In the case of the mesh configuration, the wireless network, the Independent Basic Service Set (IBSS), enables each wireless device to connect to any other wireless device within range.



### Extended Service Set (ESS)

In the cellular topology, the wireless network, referred to as an Extended Service Set (ESS),



consists of a series of overlapping wireless cells, each with its own WAP. Devices can actually move among cells and continue working seamlessly, regardless of which cell they happen to be in. It's easiest to think of this as a radio station. Imagine you're driving down a long road and you have your radio tuned to 95.5 FM. As you go along, you eventually fade out of 95.5 FM for one area, but you fade into 95.5 FM for the next area. If these two stations were playing the exact same program, you wouldn't even know that you had changed from one to another.

The ESS cascades wireless access points, enabling seamless access to data as a mobile wireless device moves along the network.

## **FACTORS WHICH AFFECT WIRELESS NETWORK RANGE SPEED INFRARED BLUETOOTH FHSS DSSS OFDM MIMO**

### Infrared

Infrared (IR) radiation is electromagnetic radiation of a wavelength longer than that of visible light, but shorter than that of microwave radiation. The name means "below red" (from the Latin infra, "below"), red being the color of visible light of longest wavelength.

## Bluetooth

Is an industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers and digital cameras via a secure, low-cost, globally available short range radio frequency.

## FHSS

Frequency-hopping spread spectrum is a spread-spectrum method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. Spread-spectrum transmission offers these advantages over a fixed-frequency transmission:

- Highly resistant to noise and interference.
- Signals are difficult to intercept. A Frequency-Hop spread-spectrum signal sounds like a momentary noise burst or simply an increase in the background noise for short Frequency-Hop codes on any narrowband receiver except a Frequency-Hop spread-spectrum receiver using the exact same channel sequence as was used by the transmitter.
- Transmissions can share a frequency band with many types of conventional transmissions with minimal interference. As a result, bandwidth can be utilized more efficiently.

## DSSS

direct-sequence spread spectrum is a modulation technique where the transmitted signal takes up more bandwidth than the information signal that is being modulated, which is the reason that it is called spread spectrum. **Direct Sequence Spread Spectrum (DSSS)** uses one



channel to send data across all frequencies within that channel. Complementary Code Keying (CCK) is a method for encoding transmissions for higher data rates, such as 5.5 and 11 Mbps, but it still allows backward compatibility with the original 802.11 standard, which supports only 1 and 2 Mbps speeds. 802.11b and 802.11g support this transmission method.

## Comparison of DSSS and Frequency Hopped SS

### DSSS

Flexible support of variable data rates  
High capacity is possible with enhancements (interference cancellation, adaptive antenna, etc.)  
Suffers from near-far effect

### FHSS

Suitable for ad hoc networks (no near-far problem)  
Robust to interference  
Limited data rate

## OFDM

Orthogonal frequency-division multiplexing, also called discrete multitone modulation (DMT), is a transmission technique based upon the idea of frequency-division multiplexing (FDM). **OFDM (Orthogonal Frequency Division Multiplexing)** increases data rates by using a spread spectrum modulation. 802.11a and 802.11g support this transmission method.

- Used in some wireless LAN applications, including WiMAX and IEEE 802.11a/g
- Used in many communications systems such as: ADSL, Wireless LAN, Digital audio broadcasting.

## MIMO (Multiple Input Multiple Output)

MIMO (Multiple Input Multiple Output) transmission, which uses DSSS and/or OFDM by spreading its signal across 14 overlapping channels at 5 MHz intervals. 802.11n uses it. Use of 802.11n requires multiple antennas.

	802.11a	802.11b	802.11g	802.11n
--	---------	---------	---------	---------

Data Rate	54 Mbps	11 Mbps	54 Mbps	248 Mbps (with 2×2 antennas)
Throughput	23 Mbps	4.3 Mbps	19 Mbps	74 Mbps
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4 and/or 5 GHz
Compatibility	None	With 802.11g and the original 802.11	With 802.11b	802.11a, b, and g
Range (meters)	35–120	38–140	38–140	70–250
Number of Channels	3	Up to 23	3	14
Transmission	OFDM	DSSS	DSSS/OFDM	MIMO

## Radio Frequency Transmission Factors

Radio frequencies (RF) are generated by antennas that propagate the waves into the air. Antennas fall under two different categories:

- Directional
- Omni-directional

**Directional** Directional antennas are commonly used in point-to-point configurations (connecting two distant buildings), and sometimes point-to-multipoint (connecting two WLANs). An example of a directional antenna is a Yagi antenna: this antenna allows you to adjust the direction and focus of the signal to intensify your range/reach.

**Omni-directional** Omni-directional antennas are used in point-to-multipoint configurations, where they distribute the wireless signal to other computers or devices in your WLAN. An access point would use an omni-directional antenna. These antennas can also be used for point-to-point connections, but they lack the distance that directional antennas supply

Three main factors influence signal distortion:

- **Absorption Objects** that absorb the RF waves, such as walls, ceilings, and floors

- **Scattering Objects** that disperse the RF waves, such as rough plaster on a wall, carpet on the floor, or drop-down ceiling tiles
- **Reflection Objects** that reflect the RF waves, such as metal and glass

### Responsible body

The International Telecommunication Union-Radio Communication Sector (ITU-R) is responsible for managing the radio frequency (RF) spectrum and satellite orbits for wireless communications: its main purpose is to provide for cooperation and coexistence of standards and implementations across country boundaries. Two standards bodies are primarily responsible for implementing WLANs:

- The Institute of Electrical and Electronic Engineers (IEEE)
- The Wi-Fi Alliance.

**IEEE** Defines the mechanical process of how WLANs are implemented in the 802.11 standards so that vendors can create compatible products.

**The Wi-Fi Alliance** Basically certifies companies by ensuring that their products follow the 802.11 standards, thus allowing customers to buy WLAN products from different vendors without having to be concerned about any compatibility issues.

### Frequencies bands:

WLANs use three unlicensed bands:

- 900 MHz Used by older cordless phones
- 2.4 GHz Used by newer cordless phones, WLANs, Bluetooth, microwaves, and other devices
- 5 GHz Used by the newest models of cordless phones and WLAN devices

900 MHz and 2.4 GHz frequencies are referred to as the Industrial, Scientific, and Medical (ISM) bands.

5 GHz frequency the Unlicensed National Information Infrastructure (UNII) band.

Unlicensed bands are still regulated by governments, which might define restrictions in their usage.

**A hertz (Hz) is a unit of frequency that measures the change in a state or cycle in a wave (sound or radio) or alternating current (electricity) during 1 second.**

### 802.11g

Suffers from the same interference as 802.11b in the already crowded 2.4 GHz range. Devices operating in this range include microwave ovens, Bluetooth devices, and cordless telephones. Since the 2.4 GHz band is heavily used, using the 5 GHz band gives 802.11a the advantage of less interference. However, this high carrier frequency also brings disadvantages. It restricts the use of 802.11a to almost line of sight, necessitating the use of more access points; it also means that 802.11a cannot penetrate as far as 802.11b since it is absorbed more readily, other things (such as power) being equal.

### 802.11a

Transmits radio signals in the frequency range above 5 GHz. This range is "regulated," meaning that 802.11a gear utilizes frequencies not used by other commercial wireless products like cordless phones. In contrast, 802.11b utilizes frequencies in the unregulated 2.4 GHz range and encounters much more radio interference from other devices.

### IEEE 802.11a / IEEE 802.11h

This is also a physical layer enhancement. IEEE 802.11a provides significantly higher performance than 802.11b, at 54 Mbps. Unlike 802.11b, the 802.11a standard operates within the frequency range of 5.47 to 5.725 GHz and is not subject to the same interference from other commercial electronic products. This higher frequency band allows significantly higher speeds of communication over the 2.4 GHz range.

802.11g APs are backward compatible with 802.11b APs. This backward compatibility with 802.11b is handled through the MAC layer, not the physical layer. On the negative side, because 802.11g operates at the same frequency as 802.11b, it is subject to the same interferences from electronic devices such as cordless phones. Since the standard's approval

in June 2003, 802.11g products are gaining momentum and will most likely become as widespread as 802.11b products. Table II-1 displays basic 802.11b/a/g characteristics.

The common range of operation for 802.11b is 150 feet for a floor divided into individual offices by concrete or sheet-rock, about 300 feet in semi-open indoor spaces such as offices partitioned into individual workspaces, and about 1000 feet in large open indoor areas. Disadvantages of 802.11b include interference from electronic products such as cordless phones and microwave ovens.

## Range

The layout of your building can reduce the range.

- A lot of concrete walls can reduce your range.
- The size of the antenna and the placement greatly affect the range of their signals
- The weather and amount of water vapor in the air can affect your signals strength

## Speed

- The layout of your building can reduce the speed
- The size of the antenna and its signal can affect your speed
- The weather and amount of water vapor can weaken the signal and affect your speed

## **MAIN FEATURES OF 802.2 LOGICAL LINK CONTROL 802.3 ETHERNET 802.5 TOKEN RING 802.11**

In this article we would discuss about media protocols, media standards. Later we would explore how system gets access over media and how topology works.

- Access method
- CSMA / CD (Carrier Sense Multiple Access / Collision Detection)
- CSMA / CA (Carrier Sense Multiple Access/Collision Avoidance)

- Topology
- Media
- Speed

## Gaining Access to the Media

Media access methods are independent of the physical and logical topologies. You will find that there are usually just a few combinations that seem to work well, however. Media access methods are simply the rules that govern how a device can submit data to the network. Each access method will have a different effect on network traffic.

## Contention as a Method of Media Access

Contention, often called random access, is the media access method that acts as an open door to anyone who wants to walk in. Two types of contention methods exist for media access; they are similar, but a single difference between them changes how efficiently they operate. They are:

- CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

## CSMA/CD

In a traditional, or hub-based, Ethernet environment, only one NIC can successfully send a frame at a time. All NICs, however, can simultaneously listen to information on the wire. Before an Ethernet NIC puts a frame on the wire, it will first sense the wire to ensure that no other frame is currently on the wire. If the cable uses copper, the NIC can detect this by examining the voltage levels on the wire. If the cable is fiber, the NIC can detect this by examining the light frequencies on the wire. The NIC must go through this sensing process, since the Ethernet medium supports

## multiple access

another NIC might already have a frame on the wire. If the NIC doesn't sense a frame on the wire, it will transmit its own frame; otherwise, if a

frame is found on the wire, the NIC will wait for the completion of the transmission of the frame and then transmit its own frame.

### Collision Detection

If two or more devices simultaneously sense the wire and see no frame, and each places its frame on the wire, a collision will occur. In this situation, the voltage levels on a copper wire or the light frequencies on a piece of fiber get messed up. For example, if two NICs attempt to put the same voltage on an electrical piece of wire, the voltage level will be different from that of only one device. Basically, the two original frames become unintelligible (or indecipherable). The NICs, when they place a frame on the wire, examine the status of the wire to ensure that a collision does not occur: this is the collision detection mechanism of CSMA/CD.

If the NICs see a collision for their transmitted frames, they have to resend the frames. In this instance, each NIC that was transmitting a frame when a collision occurred creates a special signal, called a jam signal on the wire. It then waits a small random time period, and senses the wire again. If no frame is currently on the wire, the NIC will then retransmit its original frame. The time period that the NIC waits is measured in microseconds, a delay that can't be detected by a human. Likewise, the time period the NICs wait is random to help ensure a collision won't occur again when these NICs retransmit their frames. The more devices you place on an Ethernet segment, the more likely you will experience collisions. If you put too many devices on the segment, too many collisions will occur, seriously affecting your throughput. Therefore, you need to monitor the number of collisions on each of your network segments. The more collisions you experience, the less throughput you will get.

### CSMA/CA

WLANs use a mechanism called Carrier Sense, Multiple Access/Collision Avoidance (CSMA/CA). Unlike Ethernet, it is impossible to detect collisions in a wireless medium. In a WLAN, a device cannot simultaneously send or

receive and thus cannot detect a collision: it can only do one or the other. To avoid collisions, a device will use Ready-to-Send (RTS) and Clear-to-Send (CTS) signals. When a device is ready to transmit, it first senses the airwaves for a current signal. If there is none, it generates an RTS signal, indicating that data is about to send. It then sends its data and finishes by sending a CTS signal, indicating that another wireless device can now transmit.

### Ethernet (802.3) and LLC (802.2)

There are two ways that specifications become standards. One is through standardized development, and the other is through common usage of a proprietary specification, where the usage becomes so prevalent that the specification is adopted as a standard. Ethernet is the latter. The IEEE was not the first to develop Ethernet. That honor goes to the research and development efforts of three companies in the 1970s: Digital, Intel, and Xerox, which were known collectively as DIX. Later on, the IEEE based its 802.3 standard on the DIX specification. In return, DIX updated its implementation to match the small changes made by the IEEE.

Nowadays, Ethernet is used for these and several other specifications. Ethernet 802.3 is generally implemented in conjunction with 802.2. The system uses the CSMA/CD media access method, with a logical bus topology. Physically, Ethernet can be either a star or a bus. It can use copper coaxial cabling, UTP, and fiber optics. Since Ethernet uses the broadcast system of a bus topology, each node receives every data message and examines the frame header to see whether the message is meant to be received by it. If not, the frames are discarded; if so, the frames are passed on to upper layer protocols so that the receiving application can act on them.

Data Link Layer	Name	IEEE Standard	Description
Top part	Logical Link Control (LLC)	802.2	Defines how to multiplex multiple network layer protocols in the data link layer frame, which doesn't



			have to be Ethernet. LLC is performed in software.
Bottom part	Media Access Control (MAC)	802.3	Defines how information is transmitted in an Ethernet environment and defines the framing, MAC addressing, and mechanics as to how Ethernet works. MAC is performed in hardware.

- Factors which affect Wireless Network Range Speed Infrared Bluetooth FHSS DSSS OFDM MIMO

## 10BASET 10BASEF 10BASE2 5-4-3 RULE 10BASE5 100BASEFX 100BASET4 100BASETX

IEEE shorthand identifiers, such as **10Base5**, **10Base2**, **10BaseT**, and **10BaseF** include three pieces of information:

- **The number 10:** At the front of each identifier, 10 denotes the standard data transfer speed over these media - ten megabits per second (10Mbps).
- **The word Base:** Short for Baseband, this part of the identifier signifies a type of network that uses only one carrier frequency for signaling and requires all network stations to share its use.
- **The segment type or segment length:** This part of the identifier can be a digit or a letter:
- **Digit** - shorthand for how long (in meters) a cable segment may be before attenuation sets in. For example, a 10Base5 segment can be no more than 500 meters long.
- **Letter** - identifies a specific physical type of cable. For example, the
- **T** at the end of 10BaseT stands for twisted-pair.

### 10BaseT

One of the most common types of Ethernet in use today is **10BaseT**. This particular implementation uses four-pair UTP wiring (Cat3 or higher, but most commonly you will see Cat5) using RJ-45 connectors. Each cable is connected from each network device to a central hub in a physical star topology. Within the hub, the signals are repeated and forwarded to all

other nodes on the network because it is a logical bus topology. Older network interface cards are configured with jumpers to set addresses and interrupts.

Today's network interface cards can be managed through a diagnostic program, or automatically configure themselves through plug and play technology. There is a limit of 1024 devices on an Ethernet segment, plus you can have a maximum of 1024 network segments. A UTP cable has a maximum distance of 100 meters, which is equivalent to 328 feet.

## 10BaseF

**10BaseF** is an implementation of Ethernet 802.3 over fiber optic cabling. 10BaseF offers only 10 Mbps, even though the fiber optic media has the capacity for much faster data rates. One of the implementations of 10BaseF is to connect two hubs as well as connecting hubs to workstations. The best time to use 10BaseF is in the rewiring of a network from copper to fiber optic, when you need an intermediate protocol using the new wiring. 10BaseF is not often a permanent solution because the data rate is so low and the cabling so expensive in comparison to using UTP.

## 10Base2

**10Base2**, also called ThinNet, is one of the two Ethernet specifications that use coaxial cable. (One of the best ways to remember that **10Base2** is ThinNet, and 2 is smaller than 10Base5, which is ThickNet.) One of the most important issues to remember in an Ethernet coax wiring scheme is the *5-4-3 rule*,

### **5-4-3 rule**

which states that you can have up to five cable segments, connected by four repeaters, with no more than three of these segments being mixing segments. In the days of coaxial cable networks, this meant that you could have up to three mixing segments of 500 or 185 meters each (for 10Base5 and 10Base2, respectively) populated with multiple computers and connected by two repeaters. You could also add two additional repeaters to extend the network with another two cable segments of 500

or 185 meters each, as long as these were link segments connected directly to the next repeater in line, with no intervening computers. A 10Base2 network could therefore span up to 925 meters and a 10Base5 network up to 2,500 meters which states that there can only be 5 segments in a series and 4 repeaters between these 5 segments, although only 3 of the segments can be populated with devices. 10Base2 uses BNC connectors and is implemented as both a physical and logical bus topology using RG-58 cabling.

The minimum distance for cables between workstations must be at least a half-meter. Drop cables should not be used to connect a BNC connector to the network interface card (NIC) because this will cause signaling problems unless the NIC is terminated. 10Base2 ThinNet segments cannot be longer than 185 meters, although it is often exaggerated to 200 meters, and you can't put more than 30 devices on each populated segment. The entire cabling scheme, including all five segments, can't be longer than 925 meters.

## 10Base5

**10Base5** is nearly identical to **10Base2**, except that it uses a different type of cabling and media connector. 10Base5 is known as ThickNet because it uses the RG-8 coaxial cable. It requires an external transceiver to attach to the network interface card on each device. The transceiver is a device that translates the workstation's digital signal to a baseband cabling format. ThinNet and UTP network interface cards have built-in transceivers. Only 10Base5 ThickNet network interfaces use external transceivers. In the 10Base5 configuration, the NIC attaches to the external transceiver using an AUI connector. The transceiver then clamps into the ThickNet cabling, which is why it is usually called a vampire tap. 10Base5 can also use BNC connectors. For 10Base5, the following rules apply: First the 5-4-3 rule applies to ThickNet just as it did to ThinNet. In addition, the minimum cable distance between each transceiver is 2.5 meters. The maximum network segment length is 500 meters, which is where 10Base5 gets the "5" in its name. The entire set of five segments

cannot exceed 2,500 meters. You can have 100 devices on a 10Base5 network segment.

## 100BaseFX

**100BaseFX** is simply Fast Ethernet over fiber. Originally, the specification was known as 100Base-X over CDDI (Copper Data Digital Interface) or FDDI (Fiber Data Digital Interface). Because the signaling is so vastly different, these two technologies were split into 100BaseFX and 100BaseTX. 100BaseFX runs over multimode fiber. There are two types of fiber in use. Multimode fiber optic cables use LEDs to transmit data and are thick enough that the light signals bounce off the walls of the fiber. The dispersion of the signal limits the length of multimode fiber. Single mode fiber optic cables use injected lasers to transmit the data along fiber optic cable with an extremely small diameter. Because the laser signal can travel straight without bouncing and dispersing, the signal can travel much farther than multimode.

## 100BaseT4

**100BaseT4** was the specification created to upgrade 10BaseT networks over Cat3 wiring to 100 Mbps without having to replace the wiring. Using four pairs of twisted pair wiring, two of the four pairs are configured for half-duplex transmission (data can move in only one direction at a time). The other two pairs are configured as simplex transmission, which means data moves only in one direction on a pair all the time.

## 100BaseTX

**100BaseTX**, Fast Ethernet, transmits data at 100 Mbps. Leveraging the existing IEEE 802.3u standard rules, Fast Ethernet works nearly identically to 10BaseT, including that it has a physical star topology using a logical bus. 100BaseTX requires Cat5 UTP.

## Gigabit Ethernet

The fastest form of Ethernet is currently Gigabit Ethernet, also known as 1000BaseT over Cat5 or highergrade cable, using all four pairs of the

cable. It uses a physical star topology with logical bus. There is also 1000BaseF, which runs over multimode fiber optic cabling. Data transmission is full-duplex, but half-duplex is also supported.

1.3 Specify the characteristics (For example: speed, length, topology, and cable type) of the following cable standards:

- 10BASE-T and 10BASE-FL
- 100BASE-TX and 100BASE-FX
- 1000BASE-T, 1000BASE-CX, 1000BASE-SX and 1000BASE-LX
- 10 GBASE-SR, 10 GBASE-LR and 10 GBASE-ER

Designation	Supported Media	Maximum Segment Length	Transfer Speed	Topology
<b>10Base-5</b>	Coaxial	500m	10Mbps	Bus
<b>10Base-2</b>	ThinCoaxial (RG-58 A/U)	185m	10Mbps	Bus
<b>10Base-T</b>	Category3 or above unshielded twisted-pair (UTP)	100m	10Mbps	Star,using either simple repeater hubs or Ethernet switches
<b>1Base-5</b>	Category3 UTP, or above	100m	1Mbps	Star,using simple repeater hubs
<b>10Broad-36</b>	Coaxial(RG-58 A/U CATV type)	3600m	10Mbps	Bus(often only point-to-point)
<b>10Base-FL</b>	Fiber-optic- two strands of multimode 62.5/125 fiber	2000m (full-duplex)	10Mbps	Star(often only point-to-point)
<b>100Base-TX</b>	Category5 UTP	100m	100Mbps	Star,using either simple repeater hubs or Ethernet switches
<b>100Base-FX</b>	Fiber-optic- two strands of multimode 62.5/125 fiber	412 meters (Half-Duplex) 2000 m (full-duplex)	100 Mbps (200 Mb/s full-duplex mode)	Star(often only point-to-point)

<b>1000Base-SX</b>	Fiber-optic- two strands of multimode 62.5/125 fiber	260m	1Gbps	Star,using buffered distributor hub (or point-to-point)
<b>1000Base-LX</b>	Fiber-optic- two strands of multimode 62.5/125 fiber or monomode fiber	440m (multimode) 5000 m (singlemode)	1Gbps	Star,using buffered distributor hub (or point-to-point)
<b>1000Base-CX</b>	Twinax,150-Ohm-balanced, shielded, specialty cable	25m	1Gbps	Star(or point-to-point)
<b>1000Base-T</b>	Category5	100m	1Gbps	Star

## 802.5 (token ring)

The IEEE 802.5 Token Ring standards define services for the OSI physical layer and the MAC sublayer of the data link layer. Token Ring computers are situated on a continuous network loop. A Token Ring controls access to the network by passing a token, from one computer to the next. Before they can transmit data they must wait for a free token, thus token passing does not allow two or more computers to begin transmitting at the same time.

- Token Ring has some major advantages over Ethernet:
- The maximum frame size for Token Ring is 4k, which is much more efficient than the small Ethernet maximum.
- Token Ring has long-distance capability.
- Every station in the ring is guaranteed access to the token at some point; thus, every station can transmit data.
- Error detection and recovery techniques are also enhanced in a Token Ring environment by using a monitor function normally controlled by a server. For example, if the token is lost or corrupted, the protocol provides a mechanism to generate a new token after a specified time interval has elapsed.

<b>Media</b>	<b>MAC Method</b>	<b>Signal Propagation Method</b>	<b>Speed</b>	<b>Topologies</b>	<b>Maximum Connections</b>
--------------	-------------------	----------------------------------	--------------	-------------------	----------------------------

Twisted-pair(various types)	Token passing	Forwarded from device to device (or port to port on a hub) in a closed loop	4Mbps  16 Mbps	Ring  Star-using Token Ring repeater hubs	255nodes per segment
-----------------------------	---------------	---	----------------------	---	----------------------

## 802.11b (wireless)

802.11b is a wireless Ethernet technology operating at 11MB. 802.11b devices use Direct Sequence Spread Spectrum (DSSS) radio technology operating in the 2.4GHz frequency band. An 802.11b wireless network consists of wireless NICs and access points. Access points act as wireless hubs to link multiple wireless NICs into a single subnet. Access points also have at least one fixed Ethernet port to allow the wireless network to be bridged to a traditional wired Ethernet network.. Wireless and wired devices can coexist on the same network. 802.11b devices can communicate across a maximum range of 50-300 feet from each other.

## FDDI networking technologies

Fiber Distributed Data Interface, shares many of the same features as token ring, such as a token passing, and the continuous network loop configuration. But FDDI has better fault tolerance because of its use of a dual, counter-rotating ring that enables the ring to reconfigure itself in case of a link failure. FDDI also has higher transfer speeds, 100 Mbps for FDDI, compared to 4 - 16 Mbps for Token Ring. Unlike Token Ring, which uses a star topology, FDDI uses a physical ring. Each device in the ring attaches to the adjacent device using a two stranded fiber optic cable. Data travels in one direction on the outer strand and in the other direction on the inner strand. When all devices attached to the dual ring are functioning properly, data travels on only one ring. FDDI transmits data on the second ring only in the event of a link failure.

Media	MAC Method	Signal Propagation Method	Speed	Topologies	Maximum Connections
Fiber-	Token	Forwardedfrom device to	100	Double	500 nodes

optic	passing	device (or port to port on a hub) in a closed loop	Mbps	ringStar	
-------	---------	--	------	----------	--

## TYPES OF NETWORKS LAN MAN WAN CN VPN SAN INTERNET EXTRANET INTRANET

A **network** is basically all of the components (hardware and software) involved in connecting computers across small and large distances. Networks are used to provide easy access to information, thus increasing productivity for users.

### benefits of networking

There are lots of advantages from build up a network, but the three big facts are-

#### **File** **Sharing**

From sharing files you can view, modify, and copy files stored on a different computer on the network just as easily as if they were stored on your computer.

#### **Resource** **Sharing**

Resources such as printers, fax machines, Storage Devices (HDD, FDD and CD Drives), Webcam, Scanners, Modem and many more devices can be shared.

#### **Program** **Sharing**

Just as you can share files on a network, you can often also share program on a network. For example, if you have the right type of software license, you can have a shared copy of Microsoft Office, or some other program, and keep it on the network server, from where it is also run

## Types of Networks

### Local Area Networks

**Local area networks (LANs)** are used to connect networking devices that are in a very close geographic area, such as a floor of a building, a building itself, or a campus environment.



## Wide Area Networks

**Wide area networks (WANs)** are used to connect LANs together. Typically, WANs are used when the LANs that must be connected are separated by a large distance.

## Metropolitan Area Networks

A **metropolitan area network (MAN)** is a hybrid between a LAN and a WAN.

## Storage Area Networks

**Storage area networks (SANs)** provide a high-speed infrastructure to move data between storage devices and file servers.

### Advantage

- Performance is fast.
- Availability is high because of the redundancy features available.
- Distances can span up to 10 kilometers.
- Management is easy because of the centralization of data resources.
- Overhead is low (uses a thin protocol).

Disadvantage of SANs is their cost.

## Content Networks

**Content networks (CNs)** were developed to ease users' access to Internet resources.

Companies deploy basically two types of CNs:

- caching downloaded Internet information
- Distributing Internet traffic loads across multiple servers

## Intranet

An **intranet** is basically a network that is local to a company. In other words, users from within this company can find all of their resources without having to go outside of the company. An intranet can include LANs, private WANs and MANs,

## Extranet

An **extranet** is an extended intranet, where certain internal services are made available to known external users or external business partners at remote locations.

## Internet

An **internet** is used when unknown external users need to access internal resources in your network. In other words, your company might have a web site that sells various products, and you want any external user to be able to access this service.

## VPN

A **virtual private network (VPN)** is a special type of secured network. A VPN is used to provide a secure connection across a public network, such as an internet. Extranets typically use a VPN to provide a secure connection between a company and its known external users or offices.

**Authentication** is provided to validate the identities of the two peers.

**Confidentiality** provides encryption of the data to keep it private from prying eyes.

**Integrity** is used to ensure that the data sent between the two devices or sites has not been tampered with.

## Network Media and Topologies

If you are wondering what media and topologies refer to, it all starts in the wiring closet. Media is the cabling, and topologies are the shapes that cabling and data transmissions take. Twenty percent (one-fifth) of the exam will contain questions that test your understanding of the following concepts of media and topologies.

So in this section we would presents the information needed to understand the common media used and the different types of topologies used on a network. This section covers the common media standards and the popular network components such as hubs, switches, bridges, routers, and gateways.

Wiring Tools Wire Crimper Map Testers Cable Testers Tone Generator firewall proxy

Rj-45 J Rj-11 USB MT-RJ Coaxial BNC LC Local Connector MT-RJ USB BNC connector AUI

Cable media STP UTP SMF MMF Coaxial cable ThickNet RG-8 ThinNet RG-58

## WIRING TOOLS WIRE CRIMPER MAP TESTERS CABLE TESTERS TONE GENERATOR FIREWALL PROXY

### wire crimper

A **wire crimper** is a tool that you use to attach media connectors to the ends of cables. For instance, you use one type of wire crimper to attach RJ-45 connectors on Unshielded Twisted Pair (UTP) cable, and you use a different type of wire crimper to attach Bayonet Neill Concelman (BNCs) to coaxial cabling.

### Wire Map Testers

A **wire map tester** is a device that is similar in principle to the tone generator and locator, except that it tests all the wire connections in a UTP cable at once. This device also consists of two parts, which you connect to the opposite ends of a cable. The unit at one end transmits signals over all the wires, which are detected by the unit at the other end. A wire map tester can detect transposed wires, opens, and shorts, just as a tone generator and locator can, but it does all the tests simultaneously and provides you with a simple readout telling you what's wrong.

### Multifunction Cable Testers

**Multifunction cable testers** are handheld devices, that perform a variety of tests on a cable connection and compare the results to standard values that have been programmed into the unit. The result is that these are devices that anyone can use. You simply connect the unit to the cable, press a button, and the device comes up with a list of pass or fail ratings for the individual tests. Multifunction cable testers can test any of the following:

- **Length** The most common method for determining the length of a cable is called time domain reflectometry (TDR), in which the tester transmits a signal over the cable and measures how long it takes for the signal's reflection to return. Using the nominal velocity of propagation (NVP) for the cable, which is the speed at which signals travel through the cable (supplied by the manufacturer) you can compute the length of the cable. This function also enables you to determine the location of a break in a cable.
- **Attenuation** By comparing the strength of a signal at the far end of a cable to its strength when transmitted, the tester determines the cable's attenuation (measured in decibels).
- **Near end crosstalk (NEXT)** Testing for near end crosstalk is a matter of transmitting a signal over one of a cable's wires and then detecting the strength of the signal that bleeds over into the other wires near the end of the cable where the transmitter is located.
- **Power sum NEXT (PSNEXT)** This is a measurement of the crosstalk generated when three of the four wire pairs are carrying signals at one time. This test is intended for networks using technologies like Gigabit Ethernet, which transmit signals over several wire pairs simultaneously.
- **Equal level far end crosstalk (ELFEXT)** This is a measurement of the crosstalk at the opposite end of the cable from the transmitter, corrected to account for the amount of attenuation in the connection.
- **Power sum ELFEXT (PSELFEXT)** This is a measurement of the crosstalk generated at the far end of the cable by three signal-carrying wire pairs, corrected for attenuation.
- **Propagation delay** This indicates the amount of time required for a signal to travel from one end of a cable to the other.
- **Delay skew** This is the difference between the lowest and the highest propagation delay measurements for the wires in a cable. Because the wire pairs inside a UTP cable are twisted at different rates, their relative lengths can differ, and the delay skew measurement quantifies that difference.
- **Return loss** This is a measurement of the accumulated signal reflection caused by variations in the cable's impedance along its

length. These impedance variations are typically caused by untwisting too much of the wire pairs when making connections.

## Tone Generator



One of the most basic ways to identify and test a cable connection is to use a tone generator and locator cable tester. The tone generator is a device that you connect to a cable at one end, and which transmits a signal over the cable. The tone locator is a separate device that has a probe capable of detecting the generator's signal, either by touching it to the conductor in the cable, or simply by touching it to the insulation on the outside of the cable. When the locator detects the generator's signal, it emits an audible tone. You can use this type of device to test an entire cable, or to test the individual wire connections inside a UTP cable.

Tone generators are most commonly used to identify the cable belonging to a particular connection.

### **Example:**

If you're performing an internal cable installation, and you forget to label one of your cables, you can connect the tone generator at the wall plate end and touch the probe to each of the cables at the patch panel end until you find the one that produces a tone. You can also use a tone generator and locator to test the individual wire connections inside a UTP cable.

- Connect the generator to a single wire or connector contact using alligator clips
- Then touch the locator to each wire or contact at the other end of the cable.

Using this method, you can test for any major wiring faults that affect internal UTP cable installations.

**Example:**

- If you fail to detect a signal on the contact to which you have the generator connected at the other end, you have an open circuit.
- If you detect a signal on the wrong contact, you have punched down the wires to the wrong contacts.
- If you detect a signal on two or more wires, you have a short.

**Tone generator and locator Pros:**

- Simple to use
- Most inexpensive type of cable tester
- Useful for troubleshooting a single cable connection.

**Tone generator and locator Cons:**

- Testing each of the wires in a UTP cable individually is time consuming
- You also need two people to use the equipment, one at the generator end and one at the locator end (unless you don't mind running back and forth from one end of your cable connections to the other)

**Purpose, benefits and characteristics of using a firewall.**

A firewall is a system or group of systems that enforces an access control policy between two networks. How this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms to either block or permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy.

**Firewall techniques:**

- Packet filter looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.
- Application gateway applies security mechanisms to specific applications, such as FTP and Telnet servers.
- Circuit-level gateway applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

## **Network layer firewalls**

Network layer firewalls operate at a low level of the TCP/IP protocol stack as IP-packet filters, not allowing packets to pass through the firewall unless they match the rules. The firewall administrator may define the rules; or default built-in rules may apply. Modern firewalls can filter traffic based on many packet attributes like:

- source IP address
- source port
- destination IP address or port
- destination service like WWW or FTP

They can also filter based on protocols, TTL values, netblock of originator, domain name of the source, and many other attributes.

## **Application-layer firewalls**

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets without acknowledgement to the sender. Application firewalls can prevent all unwanted outside traffic from reaching protected machines. Firewalls can't protect against attacks that don't pass through it.

## **Types of firewalls**

The term firewall is rather broad, because the features and effectiveness of any particular firewall vary greatly. However, firewalls in general can be classified into three basic forms, as outlined here:

- A dedicated hardware device

- A router with traffic filtering/firewall capabilities built in
- A software based system normally running on a server, PC, or MAC

### Purpose, benefits and characteristics of using a proxy service.

A proxy server provides numerous advantages for connecting a local area network to the Internet. Acting as an Application-Layer Gateway, the proxy provides a strong defense from the outside world. Performing the duties of a firewall, however, is just one benefit of a proxy server. The proxy can also provide caching services to increase performance, logging services to track Internet use, tools to maximize the use of precious bandwidth, and content filtering to help keep unwanted data off the local network. The proxy can also utilize multiple connection types to easily provide redundancy and automatic failover in the event of a primary line failure.

The primary security features of Proxy Server are:

- It blocks inbound connections.
- LAN clients can initiate connections to Internet servers, but Internet clients cannot initiate connections to LAN servers.
- It can restrict outbound connections.

## **RJ-45 J RJ-11 USB MT-RJ COAXIAL BNC LC LOCAL CONNECTOR MT-RJ USB BNC CONNECTOR AUI**

### RJ-11 (Registered Jack)

Standard telephone cable connectors, **RJ-11** has 4 wires (and RJ-12 has 6 wires). **RJ-11** is the acronym for Registered Jack-11, a four- or six-wire connector primarily used to connect telephone equipment.



RJ-11 Pin	Signal Name	
1	VCC (5 volts regulated)	
2	Power Ground	
3	One Wire Data	
4	One Wire Ground	

## RJ-45 (Registered Jack)

The acronym for **Registered Jack-45** is RJ-45. The **RJ-45** connector is an eight-wire connector that is commonly used to connect computers to a local area network (LAN), particularly Ethernet LANs. Although they are slightly larger than the more commonly used **RJ-11** connectors, RJ-45s can be used to connect some types of telephone equipment.



## F-Type

The **F connector** is a type of RF connector commonly used for cable and universally for satellite television. They are also used for the cable TV connection in DOCSIS cable modems, usually with RG-6 tri-shield cable. The F connector is inexpensive, yet has good performance up to 1 GHz. One reason for its low cost is that it uses the center wire of the coaxial cable as the pin of the male connector. The male connector body is typically crimped onto the exposed outer braid. Female connectors have a

3/8-32 thread. Most male connectors have a matching threaded connecting ring, though push-on versions are also available.



### ST (Straight Tip) and SC (Subscriber Connector or Standard Connector)

Fiber network segments always require two fiber cables: one for transmitting data, and one for receiving. Each end of a fiber cable is fitted with a plug that can be inserted into a network adapter, hub, or switch. In the North America, most cables use a square SC connector (Subscriber Connector or Standard Connector) that slides and locks into place when inserted into a node or connected to another fiber cable, Europeans use a round ST connector (Straight Tip) instead.



*SC connector*



*ST connector*

### Fiber LC (Local Connector)

These connectors are used for single-mode and multimode fiber-optic cables. FC connectors offer extremely precise positioning of the fiber-optic cable with respect to the transmitter's optical source emitter and the receiver's optical detector. FC connectors feature a position locatable notch and a threaded receptacle.



## MT-RJ (Mechanical Transfer Registered Jack)

**MT-RJ** connectors are used with single-mode and multimode fiber-optic cables. The **MT-RJ** connectors are constructed with a plastic housing and provide for accurate alignment via their metal guide pins and plastic ferrules.

Used for Gigabit ethernet. To connect to modules with **MT-RJ** interfaces, use multimode fiber-optic cables.



## USB (Universal Serial Bus)

Universal Serial Bus, or USB, is a computer standard designed to eliminate the guesswork in connecting peripherals to a PC. It is expected to replace serial and parallel ports. A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, keyboards, digital camera's, printers, scanners, MP3 players and many more. USB also supports Plug-and-Play installation and hot plugging.

- USB 1.1 standard supports data transfer rates of 12 Mbps.
- USB 2.0 (Also referred to as Hi-Speed USB) specification defines a new High-speed transfer rate of 480 Mb/sec.

USB 2.0 is fully compatible with USB 1.1 and uses the same cables and connectors. USB has with two connector types. The first is Type A (on the right), This connector connects to the PC's USB port. The Type B (on the left) connector and is for connecting to the relevant peripheral. Where as the type A connector is truly standard, the Type B connector could be changed in size etc. with individual peripherals meaning they require there own unique cables.



- Wiring Tools Wire Crimper Map Testers Cable Testers Tone Generator firewall proxy
- Cable media STP UTP SMF MMF Coaxial cable ThickNet RG-8 ThinNet RG-58

## **CABLE MEDIA STP UTP SMF MMF COAXIAL CABLE THICKNET RG-8 THINNET RG-58**

### STP (Shielded Twisted Pair)

This cable has a conductive braided or foil casing for each pair and theoretically offers very good protection from interference and crosstalk. It was commonly used for token ring networks.

#### *Shielded twisted pair (STP)*



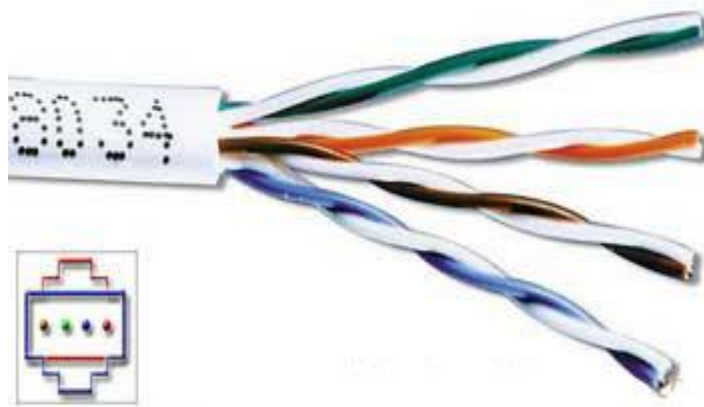
Shielded Twisted Pair is rarely used due to the fact that the potential performance increase over UTP is not worth the much greater cost of STP. STP, which is limited to 100-meter lengths (the same as UTP), is used in token ring networks and for IBM mainframe and minicomputer environments. There is no standard for it. Since token ring networks do not require STP, it is used less and less. These are few reasons for this:

- Higher cost due to greater complexity for the cabling and connectors
- Larger size and less flexibility of the cabling
- Longer installation time

### UTP (Unshielded Twisted Pair)

UTP is the most commonly used type of networking cable. UTP cables are often called "ethernet cables" after Ethernet, the most common data networking standard that utilizes UTP cables, although not the most reliable.

#### *Unshielded twisted pair (UTP)*



In contrast to FTP and STP cabling, UTP cable is not surrounded by any shielding. It is the primary wire type for telephone usage and is very common for computer networking, especially in patch cables or temporary network connections due to the high flexibility of the cables.

### Category 3

cable, commonly known as Cat-3, is an **unshielded twisted pair (UTP)** cable designed to reliably carry data up to 10 Mbit/s, with a possible bandwidth of 16 MHz. It is part of a family of copper cabling standards defined jointly by the Electronic Industries Alliance and the Telecommunications Industry Association. Category 3 was a popular cabling format among computer network administrators in the early 1990s, but has since been almost entirely replaced by the very similar Cat-5 standard, which offers higher top speeds.

### Category 5

Cable, commonly known as Cat 5, is an unshielded twisted pair type cable designed for high signal integrity. The actual standard defines specific electrical properties of the wire, but it is most commonly known as being rated for its Ethernet capability of 100 Mbit/s. Its specific standard designation is EIA/TIA-568. Cat 5 cable typically has three twists per inch of each twisted pair of 24 gauge copper wires within the cable. The twisting of the cable reduces electrical interference and crosstalk.

Another important characteristic is that the wires are insulated with a plastic (FEP) that has low dispersion, that is, the dielectric constant of the plastic does not depend greatly on frequency. Special attention also has to be paid to minimizing impedance mismatches at connection points.

Cat 5 cables are often used in structured cabling for computer networks such as Fast Ethernet, although they are also used to carry many other signals such as basic voice services, token ring, and ATM (at up to 155 Mbit/s, over short distances).

### Category 5e

cable is an enhanced version of Cat 5 for use with 1000BASE-T (gigabit) networks, or for long-distance 100 Base-T links (350 m, compared with 100 m for Cat 5). It must meet the EIA/TIA 568A-5 specification. Virtually all cables sold as Cat 5 are actually Cat 5e. The markings on the cable itself reveal the exact type.

### Category 6

A cable standard for Gigabit Ethernet and other interconnect that is backward compatible with Category 5 cable, Cat-5e and Cat-3. Cat-6 features more stringent specifications for crosstalk and system noise. The cable standard is suitable for 10BASE-T / 100BASE-TX and 1000BASE-T (Gigabit Ethernet) connections.

The cable contains four twisted copper wire pairs, just like earlier copper cable standards, although each twisted pair is made up of slightly larger 23 gauge copper wire as opposed to Cat 5's 24 gauge wire. When used as a patch cable, Cat-6 is normally terminated in RJ-45 electrical connectors. If components of the various cable standards are intermixed, the performance of the signal path will be limited to that of the lowest category. The distance without losing data is 220 m.

### Category 7

(CAT7), (ISO/IEC 11801:2002 category 7/class F), is a cable standard for Ultra Fast Ethernet and other interconnect technologies that can be made to be backwards compatible with traditional CAT5 and CAT6 Ethernet cable. CAT7 features even more stringent specifications for crosstalk and system noise than CAT6. To achieve this, shielding has been added for individual wire pairs and the cable as a whole.

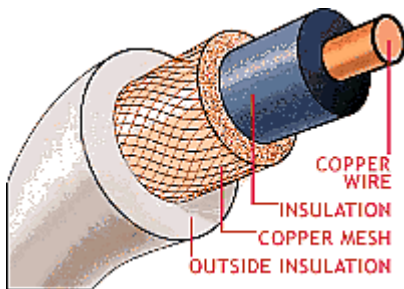
The CAT7 cable standard has been created to allow 10-gigabit Ethernet over 100 m of copper cabling. The cable contains four twisted copper wire pairs, just like the earlier standards. CAT7 can be terminated in RJ-45 compatible GG45 electrical connectors which incorporate the RJ-45 standard, and a new type of connection to enable a smoother migration to the new standard. When combined with GG-45 connectors, CAT7 cable is rated for transmission frequencies of up to 600 MHz.

### Coaxial cable

Coaxial cable is an electrical cable consisting of a round conducting wire, surrounded by an insulating spacer, surrounded by a cylindrical conducting sheath, and usually surrounded by a final insulating layer.



Most common use of coax (the short form of coaxial cable) today is in standard cable TV. If you have the chance to examine a cable, you will find that it has a fairly simple design. A copper conductor lies in the center of the cable, which is surrounded by insulation. A braided or mesh outer covering surrounds the insulation. This is also a conductor.



A PVC plastic jacket encases the covering. The cable is designed to carry a high-frequency or broadband signal, as a high-frequency transmission line. Because the electromagnetic field carrying the signal exists (ideally) only in the space between the inner and outer conductors, it cannot interfere with or suffer interference from external electromagnetic fields.

### ThickNet, or RG-8,

is older and one of the first types of coaxial cable used in networks. RG-8 is strung in a physical bus topology. Its thick shielding makes it fairly immune to noise but also very rigid and difficult to work with. RG-8 requires connectors, called vampire taps, that pierce through its thick outer shielding. Both ends of the bus must be terminated with a 50-ohm resistor; without both functioning resistors, the network will fail.

### ThinNet or RG-58

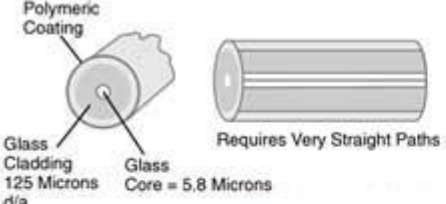
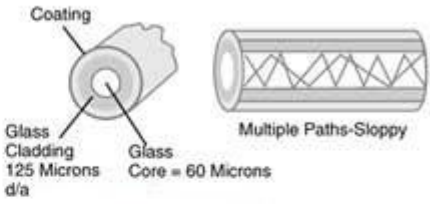
cable is far more flexible than ThickNet and much easier to work with. RG-58 cabling is also strung as a physical bus. It is capable of connecting a maximum of 30 devices on up to a 185-meter length of cable. ThinNet is constructed like ThickNet, except that the central conductor and the insulation are much thinner. British Naval Connectors (BNCs) are crimped onto the cable for connectivity, and 50-ohm resistors are required at each



end of the cable. They used to be common for implementing computer networks, in particular Ethernet, but twisted pair cables have replaced them in most applications.

## SMF (Single Mode Fiber) optic cable

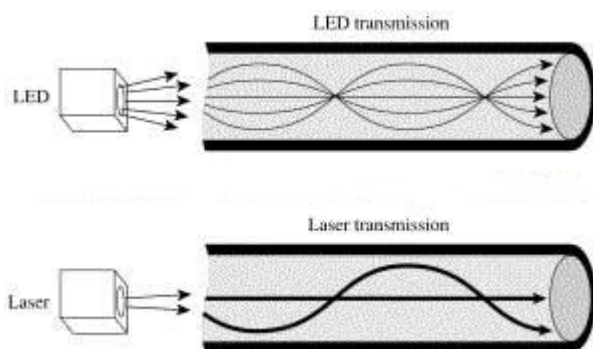
Single-mode optical fiber is an optical fiber in which only the lowest order bound mode can propagate at the wavelength of interest. Single mode fibers are best at retaining the fidelity of each light pulse over longer distances and exhibit no dispersion caused by multiple spatial modes; thus more information can be transmitted per unit time giving single mode fibers a higher bandwidth in comparison with multi-mode fibers. A typical single mode optical fiber has a core radius of 5-10 micrometers and a cladding radius of 120 micrometers. Currently, data rates of up to 10 Gigabits/second are possible at distances of over 60 km with commercially available transceivers. Equipment for Single mode fiber is more expensive than equipment for Multi-mode optical fiber, but the single mode fiber itself is usually cheaper in bulk.

Single-Mode	Multimode
	
<ul style="list-style-type: none"> <li>• Small Core</li> <li>• Less Dispersion</li> <li>• Suited for Long-Distance Applications (Up to ~ 3 km)</li> <li>• Uses Lasers as the Light Source Often Within Campus Backbones for Distances of Several Thousand Meters</li> </ul>	<ul style="list-style-type: none"> <li>• Larger Core Than Single-Mode Cable (50 Microns or Greater)</li> <li>• Allows Greater Dispersion and, Therefore, Loss of Signal</li> <li>• Used for Long-Distance Application, but Shorter Than Single-Mode (Up to ~ 2 km)</li> <li>• Uses LEDs as the Light Source Often Within LANs or Distances of a Couple Hundred Meters Within a Campus Network</li> </ul>

## MMF (Multimode Fiber) optic cable

Multi-mode optical fiber (multimode fiber or MM fiber) is a type of optical fiber mostly used for communication over shorter distances, e.g. within a

building. It can carry 1 Gbit/s for typical building distances; the actual maximum speed depends upon the distance. It is easier to connect to than single-mode optical fiber, but its limit on speed. Multi-mode fiber has a larger center core than single-mode fiber, which allows it to support more than one propagation mode, or path within the fiber. The equipment used for communications over multi-mode optical fiber is less expensive than that for single-mode optical fiber. Typical transmission speeds/distances limits are 100 Mbit/s up to 2 km (100BASE-FX), 1 Gbit/s for distances up to 500-600 meters (1000BASE-LX, 1000BASE-SX), and 10 Gbit/s for distances up to 300 meters (10GBASE-SR).



- Rj-45 J Rj-11 USB MT-RJ Coaxial BNC LC Local Connector MT-RJ USB BNC connector AUI

## CABLE MEDIA STP UTP SMF MMF COAXIAL CABLE THICKNET RG-8 THINNET RG-58

### STP (Shielded Twisted Pair)

This cable has a conductive braided or foil casing for each pair and theoretically offers very good protection from interference and crosstalk. It was commonly used for token ring networks.

#### Shielded twisted pair (STP)



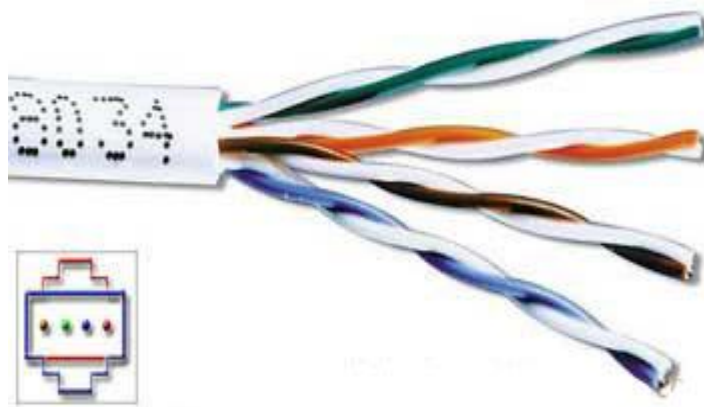
Shielded Twisted Pair is rarely used due to the fact that the potential performance increase over UTP is not worth the much greater cost of STP. STP, which is limited to 100-meter lengths (the same as UTP), is used in token ring networks and for IBM mainframe and minicomputer environments. There is no standard for it. Since token ring networks do not require STP, it is used less and less. These are few reasons for this:

- Higher cost due to greater complexity for the cabling and connectors
- Larger size and less flexibility of the cabling
- Longer installation time

### UTP (Unshielded Twisted Pair)

UTP is the most commonly used type of networking cable. UTP cables are often called "ethernet cables" after Ethernet, the most common data networking standard that utilizes UTP cables, although not the most reliable.

#### *Unshielded twisted pair (UTP)*



In contrast to FTP and STP cabling, UTP cable is not surrounded by any shielding. It is the primary wire type for telephone usage and is very common for computer networking, especially in patch cables or temporary network connections due to the high flexibility of the cables.

### Category 3

cable, commonly known as Cat-3, is an **unshielded twisted pair (UTP)** cable designed to reliably carry data up to 10 Mbit/s, with a possible bandwidth of 16 MHz. It is part of a family of copper cabling standards defined jointly by the Electronic Industries Alliance and the Telecommunications Industry Association. Category 3 was a popular cabling format among computer network administrators in the early 1990s, but has since been almost entirely replaced by the very similar Cat-5 standard, which offers higher top speeds.

### Category 5

Cable, commonly known as Cat 5, is an unshielded twisted pair type cable designed for high signal integrity. The actual standard defines specific electrical properties of the wire, but it is most commonly known as being rated for its Ethernet capability of 100 Mbit/s. Its specific standard designation is EIA/TIA-568. Cat 5 cable typically has three twists per inch of each twisted pair of 24 gauge copper wires within the cable. The twisting of the cable reduces electrical interference and crosstalk.

Another important characteristic is that the wires are insulated with a plastic (FEP) that has low dispersion, that is, the dielectric constant of the plastic does not depend greatly on frequency. Special attention also has to be paid to minimizing impedance mismatches at connection points.

Cat 5 cables are often used in structured cabling for computer networks such as Fast Ethernet, although they are also used to carry many other signals such as basic voice services, token ring, and ATM (at up to 155 Mbit/s, over short distances).

### Category 5e

cable is an enhanced version of Cat 5 for use with 1000BASE-T (gigabit) networks, or for long-distance 100 Base-T links (350 m, compared with 100 m for Cat 5). It must meet the EIA/TIA 568A-5 specification. Virtually all cables sold as Cat 5 are actually Cat 5e. The markings on the cable itself reveal the exact type.

### Category 6

A cable standard for Gigabit Ethernet and other interconnect that is backward compatible with Category 5 cable, Cat-5e and Cat-3. Cat-6 features more stringent specifications for crosstalk and system noise. The cable standard is suitable for 10BASE-T / 100BASE-TX and 1000BASE-T (Gigabit Ethernet) connections.

The cable contains four twisted copper wire pairs, just like earlier copper cable standards, although each twisted pair is made up of slightly larger 23 gauge copper wire as opposed to Cat 5's 24 gauge wire. When used as a patch cable, Cat-6 is normally terminated in RJ-45 electrical connectors. If components of the various cable standards are intermixed, the performance of the signal path will be limited to that of the lowest category. The distance without losing data is 220 m.

### Category 7

(CAT7), (ISO/IEC 11801:2002 category 7/class F), is a cable standard for Ultra Fast Ethernet and other interconnect technologies that can be made to be backwards compatible with traditional CAT5 and CAT6 Ethernet cable. CAT7 features even more stringent specifications for crosstalk and system noise than CAT6. To achieve this, shielding has been added for individual wire pairs and the cable as a whole.

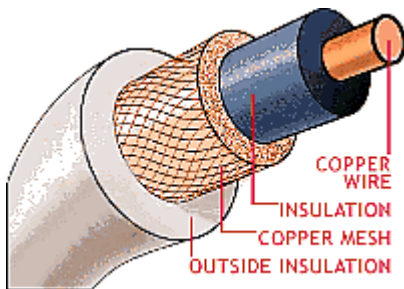
The CAT7 cable standard has been created to allow 10-gigabit Ethernet over 100 m of copper cabling. The cable contains four twisted copper wire pairs, just like the earlier standards. CAT7 can be terminated in RJ-45 compatible GG45 electrical connectors which incorporate the RJ-45 standard, and a new type of connection to enable a smoother migration to the new standard. When combined with GG-45 connectors, CAT7 cable is rated for transmission frequencies of up to 600 MHz.

### Coaxial cable

Coaxial cable is an electrical cable consisting of a round conducting wire, surrounded by an insulating spacer, surrounded by a cylindrical conducting sheath, and usually surrounded by a final insulating layer.



Most common use of coax (the short form of coaxial cable) today is in standard cable TV. If you have the chance to examine a cable, you will find that it has a fairly simple design. A copper conductor lies in the center of the cable, which is surrounded by insulation. A braided or mesh outer covering surrounds the insulation. This is also a conductor.



A PVC plastic jacket encases the covering. The cable is designed to carry a high-frequency or broadband signal, as a high-frequency transmission line. Because the electromagnetic field carrying the signal exists (ideally) only in the space between the inner and outer conductors, it cannot interfere with or suffer interference from external electromagnetic fields.

### ThickNet, or RG-8,

is older and one of the first types of coaxial cable used in networks. RG-8 is strung in a physical bus topology. Its thick shielding makes it fairly immune to noise but also very rigid and difficult to work with. RG-8 requires connectors, called vampire taps, that pierce through its thick outer shielding. Both ends of the bus must be terminated with a 50-ohm resistor; without both functioning resistors, the network will fail.

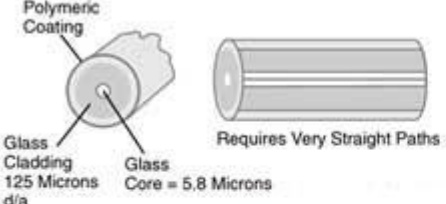
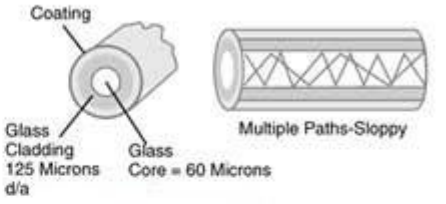
### ThinNet or RG-58

cable is far more flexible than ThickNet and much easier to work with. RG-58 cabling is also strung as a physical bus. It is capable of connecting a maximum of 30 devices on up to a 185-meter length of cable. ThinNet is constructed like ThickNet, except that the central conductor and the insulation are much thinner. British Naval Connectors (BNCs) are crimped onto the cable for connectivity, and 50-ohm resistors are required at each

end of the cable. They used to be common for implementing computer networks, in particular Ethernet, but twisted pair cables have replaced them in most applications.

## SMF (Single Mode Fiber) optic cable

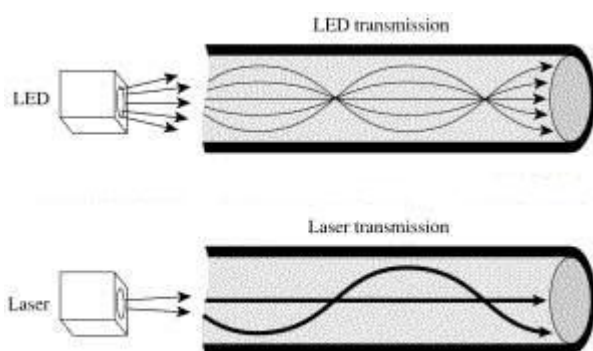
Single-mode optical fiber is an optical fiber in which only the lowest order bound mode can propagate at the wavelength of interest. Single mode fibers are best at retaining the fidelity of each light pulse over longer distances and exhibit no dispersion caused by multiple spatial modes; thus more information can be transmitted per unit time giving single mode fibers a higher bandwidth in comparison with multi-mode fibers. A typical single mode optical fiber has a core radius of 5-10 micrometers and a cladding radius of 120 micrometers. Currently, data rates of up to 10 Gigabits/second are possible at distances of over 60 km with commercially available transceivers. Equipment for Single mode fiber is more expensive than equipment for Multi-mode optical fiber, but the single mode fiber itself is usually cheaper in bulk.

Single-Mode	Multimode
 <p>Polymeric Coating</p> <p>Glass Cladding 125 Microns d/a</p> <p>Glass Core = 5.8 Microns</p> <p>Requires Very Straight Paths</p>	 <p>Coating</p> <p>Glass Cladding 125 Microns d/a</p> <p>Glass Core = 60 Microns</p> <p>Multiple Paths-Sloppy</p>
<ul style="list-style-type: none"><li>• Small Core</li><li>• Less Dispersion</li><li>• Suited for Long-Distance Applications (Up to ~ 3 km)</li><li>• Uses Lasers as the Light Source Often Within Campus Backbones for Distances of Several Thousand Meters</li></ul>	<ul style="list-style-type: none"><li>• Larger Core Than Single-Mode Cable (50 Microns or Greater)</li><li>• Allows Greater Dispersion and, Therefore, Loss of Signal</li><li>• Used for Long-Distance Application, but Shorter Than Single-Mode (Up to ~ 2 km)</li><li>• Uses LEDs as the Light Source Often Within LANs or Distances of a Couple Hundred Meters Within a Campus Network</li></ul>

## MMF (Multimode Fiber) optic cable

Multi-mode optical fiber (multimode fiber or MM fiber) is a type of optical fiber mostly used for communication over shorter distances, e.g. within a

building. It can carry 1 Gbit/s for typical building distances; the actual maximum speed depends upon the distance. It is easier to connect to than single-mode optical fiber, but its limit on speed. Multi-mode fiber has a larger center core than single-mode fiber, which allows it to support more than one propagation mode, or path within the fiber. The equipment used for communications over multi-mode optical fiber is less expensive than that for single-mode optical fiber. Typical transmission speeds/distances limits are 100 Mbit/s up to 2 km (100BASE-FX), 1 Gbit/s for distances up to 500-600 meters (1000BASE-LX, 1000BASE-SX), and 10 Gbit/s for distances up to 300 meters (10GBASE-SR).



- [Rj-45 J Rj-11 USB MT-RJ Coaxial BNC LC Local Connector MT-RJ USB BNC connector AUI](#)

## COMPUTER HARDWARE REVIEW AND DEFINITION

Network administrator must be familiar with basic computer hardware operations. He should have adequate knowledge of computer hardware to perform day by day task. So in this article we would cover some basic computer hardware terms. This could also be helpful for interview.

### What is a Computer?

- An electronic machine
  - o that can be programmed to
  - o accept data (input), and
  - o process it into
  - o useful information (output).
- Kept in secondary storage (storage) for safekeeping or later use.



- The processing of input into output is directed by the software, but performed by the hardware.

## The System Unit

The System Unit houses the central processing unit, memory modules, expansion slots, and electronic circuitry as well as expansion cards that are all attached to the motherboard; along with disk drives, a fan or fans to keep it cool, and the power supply.

All other devices (monitor, keyboard, mouse, etc., are linked either directly or indirectly into the system unit.)

## The Motherboard

The **motherboard** is the main circuit board of a computer. It contains the central processing unit (CPU), the Basic Input/Output System (BIOS), memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers for standard peripheral devices like the keyboard, disk drive and display screen.

The **chipset** is a critical part of any computer, because it plays a big role in determining what sorts of features the computer can support.

## Hardware components

### **Input devices -**

accept data or commands in a form useable by computers

### **Output devices**

display the processed information - printers, monitors, speakers.

### **Processing devices**

In system unit and are comprised of circuitry.

### **Storage devices -**

Drives read from and write to storage media (the physical material that can store data and programs).

### **Communication devices**

provide connections between computers and communication networks, allowing for exchange of information and data with other computers via transmission media such as cables, telephone lines, and satellites

In this article we would cover basic of computer hardware. Being a system administrator you should familiar with computer hardware terminology.

## The Motherboard

The **motherboard** is the main circuit board of a computer. It contains the central processing unit (CPU), the Basic Input/Output System (BIOS), memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers for standard peripheral devices like the keyboard, disk drive and display screen.

The **chipset** and other motherboard circuitry are the "smarts" of the motherboard. Their job is to direct traffic and control the flow of information inside the computer.

The **chipset** is a critical part of any computer, because it plays a big role in determining what sorts of features the computer can support.



## BIOS

- **BIOS** stands for Basic Input/Output System.
- lowest-level software in the computer

- Acts as an interface between the hardware (especially the chipset and processor) and the operating system.
- The BIOS provides access to the system hardware and enables the creation of the higher-level operating systems that you use to run your applications.
- The BIOS is also responsible for allowing you to control your computer's hardware settings, for booting up the machine when you turn on the power or hit the reset button, and various other system functions.

## ROM: Read Only Memory

- **ROM** is nonvolatile. ROM chips contain permanently written data, called firmware (your BIOS lives here).
- **ROM** contains the programs that direct the computer to load the operating system and related files when the computer is powered on.
- **ROM** chips are usually recorded when they are manufactured.

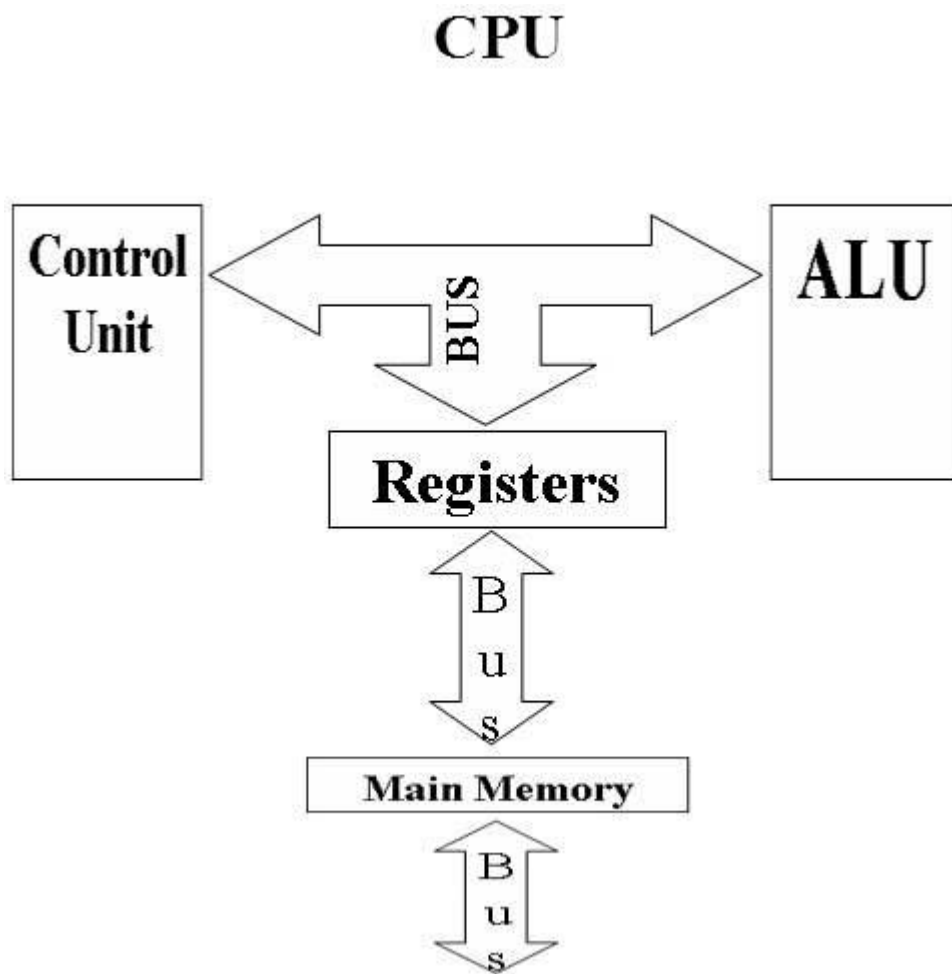
**PROM** -Programmable Read Only memory chip cannot be changed to update or revise the program inside

**EPROM** Erasable Programmable Read Only memory Data can be erased and chip can be reused Can be erased by shining high intensity UV light through the window

**EEPROM** Electrical Erasable Programmable Read Only memory under high voltage

**FROM** -Flash ROM is reprogrammable memory using normal voltage inside the PC- You can upgrade the logic capabilities by simply downloading new software. This saves the expense of replacing circuit boards and chips.

## Processing Devices



## Cache

Pronounced cash.

It is a small, high-speed memory area that is placed between the processor and the system memory.

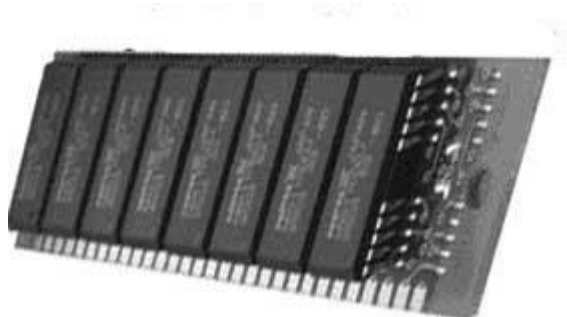
The value of the cache is that it is much faster than normal system memory.

The most frequently used instructions are kept in cache memory so that the CPU can look in there first - allows the CPU to run faster because it doesn't have to take time to swap instructions in and out of main memory.

Large, complex programs such as complex spreadsheets or database management programs benefit the most from having a cache memory available. Pentium II processors generally come with at least 512 KB of cache memory.

## Random Access Memory (RAM)

- **RAM** is Primary Storage, also called internal storage.
- Serves as computers workspace, storing all or part of the program that is being executed, as well as data being used by the program.
- **RAM** provides instructions and data to the CPU.
- These instructions/data are coded in bytes.
- Each byte is placed in a precise location in memory, called an address.
- To access data or instructions in memory, the computer references the addresses containing the bytes.
- The amount of memory available is therefore measured in bytes



- **RAM** chips consist of millions of switches that are sensitive to changes in electric current.
  - **RAM** chips are typically packaged on small circuit boards called memory modules, which are inserted into special slots on the motherboard.
  - **RAM** is Volatile storage: Power goes, data goes!
  - Data/instructions are copied into memory as needed.
  - Not enough memory or corruption of data/instructions in memory can cause crash.
  - On booting, operating system files are loaded from a storage device (the hard disk, usually) into RAM, and they remain there as long as your computer is running.
  - **RAM** contents changes as programs are executed.
- 
- RAM chips consist of millions of switches that are sensitive to changes in electric current.
  - RAM chips are typically packaged on small circuit boards called memory modules, which are inserted into special slots on the motherboard.

- On booting, operating system files are loaded from a storage device (the hard disk, usually) into RAM, and they remain there as long as your computer is running.
- RAM contents changes as programs are executed.
- The amount of RAM needed depends on the types of applications you intend to run on the computer. S/w indicate the minimum amount of RAM required to run.

Two basic types of RAM are Dynamic RAM (DRAM), and Static RAM (SRAM).

Most computers today use DRAM, which are also of two types:

- SDRAM Synchronous Dynamic RAM runs at the same pace as the system clock runs
- DDR SDRAM DDR stands for Double Data Rate - runs at double the pace the system clock runs - available in speeds from 266 MHZ upto 600MHZ
- DDR2 SDRAM runs at four times the pace the system clock runs - available in speeds from 400 MHZ upto 800MHZ

Most desktops and notebooks use one of the three most popular types of synchronous dynamic random access memory (SDRAM) for the main system memory. Single data rate (SDR) SDRAM is the older type of memory, commonly used in computers prior to 2002. Double data rate (DDR) SDRAM hit the mainstream computer market around 2002, and DDR2-based systems hit the market in mid-2004.

**DDR SDRAM** is a straightforward evolution from SDR SDRAM. The big difference between DDR SDRAM and SDR SDRAM is that DDR reads data on both the rising and falling edges of the clock signal, so the DDR module can transfer data twice as fast as SDR SDRAM.

While **DDR** has a limited clock rate, the evolutionary changes to DDR architecture enable DDR2 to achieve speeds beyond of DDR, delivering bandwidth of 5.3 GB per second and beyond! Because DDR2 is able to operate with faster bus speeds, your memory doesn't hold back the performance of your processor.

Generally speaking, motherboards are built to support only one type of memory. You cannot mix and match SDRAM, DDR, or DDR2 memory on the same motherboard in any system. They will not function and will not even fit in the same.

## Why is RAM so important?

Aside from the processor, the two most important factors affecting a PC's performance are RAM and hard disk capacity.

Hard disks are typically huge, so the primary limiting factor is the amount of installed RAM.

Without enough RAM, the operating system must swap out storage space with the hard disk. The OS creates a Paging File (swap file) to supplement RAM (workspace). This is Virtual Memory.

Virtual memory is inherently slow! RAM speed can typically be 120,000 times FASTER than the hard disk so the less you must rely on virtual memory (swapping files between RAM and hard disk), the faster your system will perform.

## Microprocessor

- Heart and brain of the PC
- One electrical circuit in control of another
- Successive generation of processors
- 80286,80386,80486 -32 bit interface
- Pentium family P1, P2, P3, P4 64 bit interface
- Dual-core technology is like having two processors - A dual core processor is a CPU with two separate cores residing on the same chip

## **DEFINITIONS COMPUTERS HARDWARE BASIC CODING SCHEMES COMPUTER PERIPHERALS**

In this article we would discuss about coding schemes used in computer, definition of computer. Later we would cover measurement unit used in computer storages.

## What is a Computer?

- An electronic machine
  - that can be programmed to
  - accept data (input), and
  - process it into

- useful information (output).
- Kept in secondary storage (storage) for safekeeping or later use.
- The processing of input into output is directed by the software, but performed by the hardware.



## Bits & Bytes

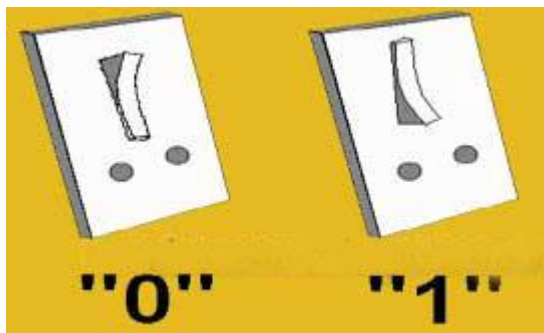
Computers are devices powered by electricity, which has two discrete states:

On

or

Off.

Two digits represent these states:



- To be processed, all data in a computer system (words, symbols, pictures, videos, sounds) must be reduced to a string of binary digits.
- A binary digit 1 or 0 is called a bit,
- Eight bits grouped together as a unit are called a byte, which provides enough combinations of 0s and 1s to represent 256 individual characters, including numbers, upper and lower case alphabet letters, punctuation marks and other characters

Name	Abb	Approx. Bytes	Exact Bytes	Approx. Pages of
------	-----	---------------	-------------	------------------



				<b>Text</b>
Byte	B	One	1	One character
Kilobyte	KB (or K)	One thousand	1,024	One-half page
Megabyte	MB	One million	1,048,576	500 pages
Gigabyte	GB	One billion	1,073,741,824	500,000 pages
Terabyte	TB	One trillion	1,099,511,627,776	500,000,000 pages

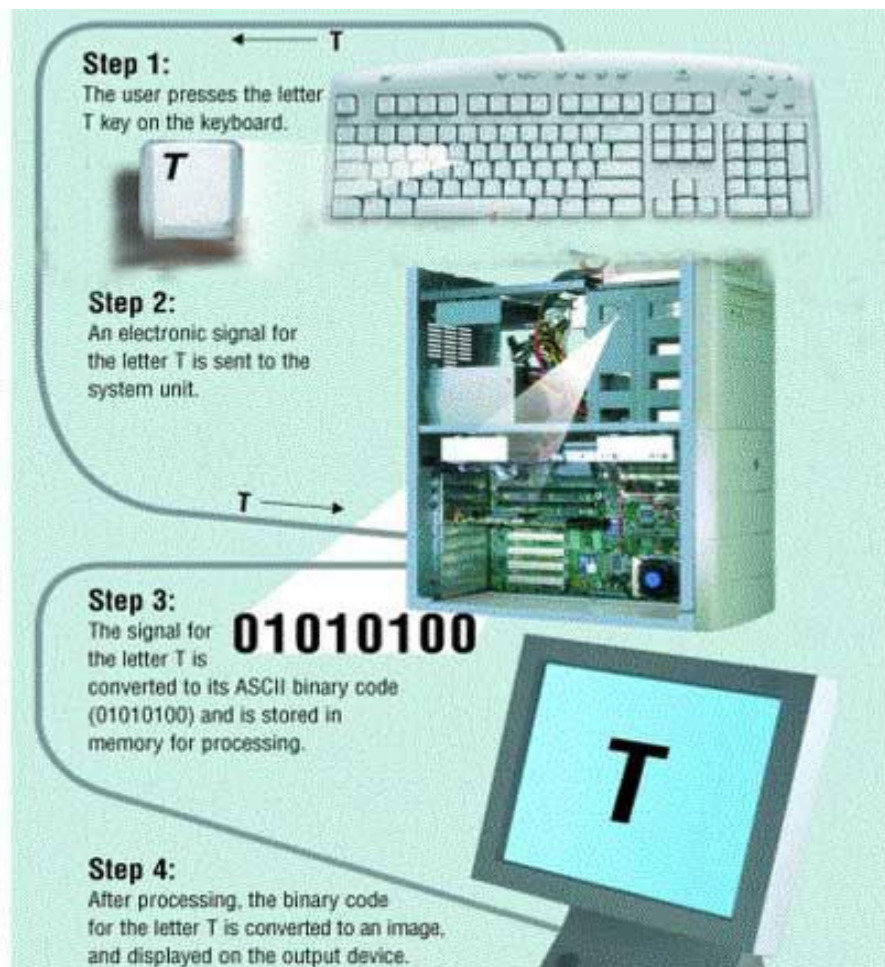
## Coding Schemes

Define the patterns of bytes

Coding schemes, such as ASCII, EBCDIC, and Unicode, provide the means to interact with a computer

When a letter is pressed on a keyboard, the electronic signals are converted into binary form and stored into memory.

The computer processes the data as bytes of information and converts them to the letters we see on the monitor screen or on a printed page.



## Terminology

- **Hardware (H/w)** All machinery & Equipments Computer & Peripherals
- **Peripherals** Any piece of hardware connected to the PC
- **Software (S/w)** programs- tells the Computer how to perform a task
  - **Systems Software (S/w)** For managing internal activities & run applications s/w Interpreter bet S/w & H/w
  - **Application Software (S/w)** - to perform a specific task Custom or Packaged

I have given a brief over view about computer hardware terminology in our last article. Now in this article I would discuss about hardware components of computer.

## Hardware components

### **Input devices -**

accept data or commands in a form useable by computers

### **Output devices**

display the processed information - printers, monitors, speakers.

## Processing devices

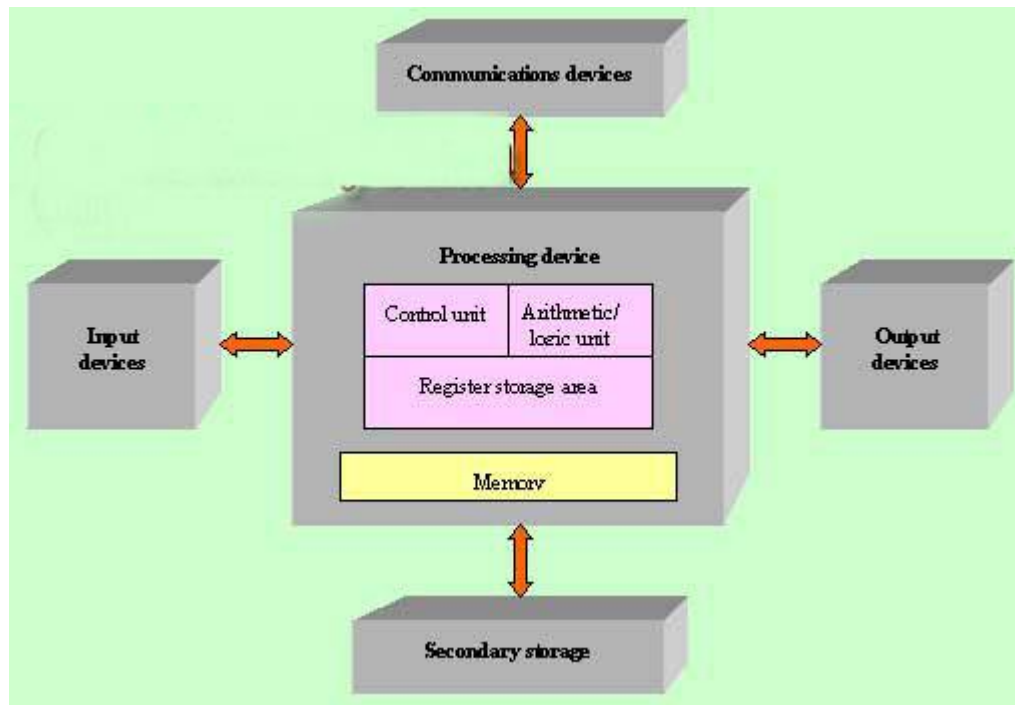
in system unit and are comprised of circuitry.

## Storage devices -

Drives read from and write to storage media (the physical material that can store data and programs).

## Communication devices

provide connections between computers and communication networks, allowing for exchange of information and data with other computers via transmission media such as cables, telephone lines, and satellites



## Input Devices

- Keyboards
- Pointing Devices mouse, trackballs, joysticks, touchpads and light pens
- Source Entry devices Scanners, Audio input devices, video input devices, digital cameras

## Output Devices

### Softcopy

Monitor /Display Screens CRT and Flat Panel (LCD), EL and gas plasma

### Monitor /Display Screen clarity

#### Resolution

refers to the number of dots displayed in the X (across) and Y (down) co-ordinates.

expressed in terms of horizontal pixels X vertical pixels.

Typical screens are capable of displaying 640x480 dots

#### Dot

#### Pitch

measurement of how close together the pixels, or phosphor dots, are that make up an image.

The smaller the dot pitch, the crisper the image, 0.31 or less provides a sharp image, especially when displaying text.

### **Refresh rate**

the vertical frequency, or the rate at which each pixel on a screen is redrawn. A low refresh rate results in an image that flickers, resulting in eye-strain.

A refresh rate of 60Hz means the image is redrawn 60 times a second. Typical refresh rates are 60Hz, 72Hz and 75Hz.

### Video Display Adapters

**Display graphics** - Visual output from your system.

Works between the system's processor and monitor

Relays the information received from the programs and applications running on the system to the monitor

**VDAs** come with their own memory chips (RAM or VRAM for video RAM) which determines how fast the card processes images, the resolution, and how many colours it can display.

**VDA** embody certain standards.

Today's PCs commonly use VGA and SVGA standards

### Hardcopy Output : Printers

#### Impact Printers

The general features of impact printers are uses force by applying hammer pins to strike the paper

- slow speed
- prints on most paper types
- transparencies not supported
- multiple copies may be printed at once

**Advantages :** Less expensive, Fast (some types) , Can make multiple copies with multipart paper

**Disadvantages :** Noisy! Print quality lower in some types. Poor graphics or none at all.

## Dot-Matrix and Daisy-Wheel.

**Dot matrix printers** form characters using row(s) of pins, 9, 18, or 24 which impact the ribbon on top of the paper.

**Daisy wheel printers** use a spoked wheel with characters placed at the end of each spoke. A print hammer is used to strike the desired character onto the ink ribbon and then the paper.

## Hardcopy Output : Printers

### Non Impact Printers

General features print head does not make contact with the paper

- higher speed in characters per second is possible
- prints on most paper types but better quality obtained with better paper
- transparencies usually supported
- Uses ink spray or toner powder
- Offer superior quality and greater options (in terms of the number of fonts and quality of graphic pictures)

**Disadvantages :** more expensive.

The three main types of non-impact printers are laserjet, inkjet and thermal

### Characters of printers

**Speed:** The speed of a printer is measured in: cps= characters per second, lpm= lines per minute ppm= pages per minute The faster the printing, the more expensive the printer.

**Resolution:** A more numerical measure of print quality is printer resolution. Measured in dots per inch (dpi), this determines how smooth a diagonal line the printer can produce.

### Cable connection:

**Serial Cables-** send data only 1 bit at a time- Distance from PC 1000 ft

**Parallel Cables-** send data 8 bits at a time. Distance from PC 50 ft.-  
Most popular - USB cable which has a maximum data transfer speed of 12 megabits/s (1.5 MBYTES/s).

## **EXAMPLES OF COMPUTER HARDWARE SYSTEM UNIT TYPES OF PORTS TYPES OF CONNECTORS**

In this article I would give you a brief overview about system unit, type of port and type of connector.

### The System Unit

The System Unit houses the central processing unit, memory modules, expansion slots, and electronic circuitry as well as expansion cards that are all attached to the motherboard; along with disk drives, a fan or fans to keep it cool, and the power supply.

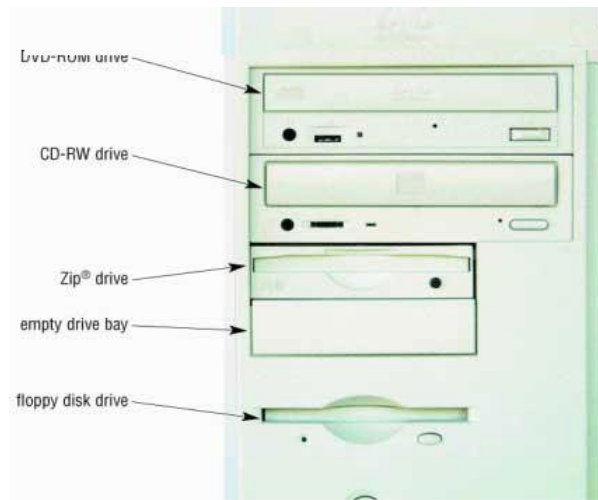
All other devices (monitor, keyboard, mouse, etc., are linked either directly or indirectly into the system unit.



### Front of the System Unit

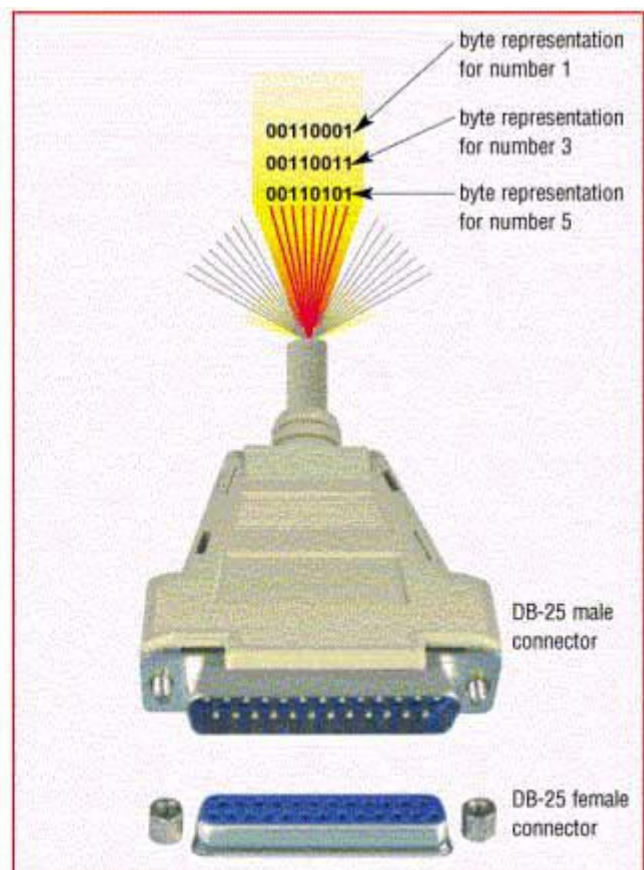
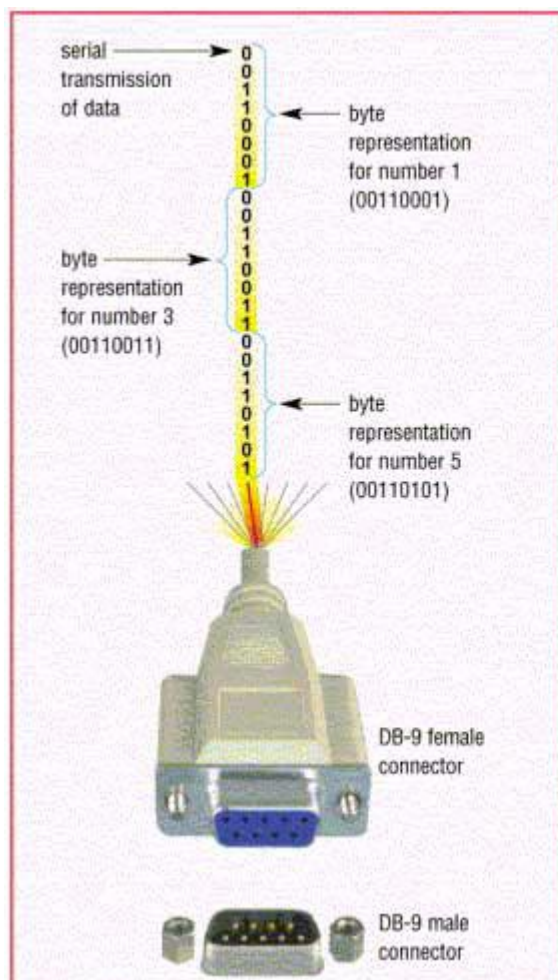
Drives are housed in drive bays which are accessed at the front of the case.

Internal drives, such as the hard disk drive, are installed in internal bays that are not typically as accessible as the external drives pictured here.



System Unit cases come in a huge array of types and styles, depending upon hardware needs.

## Types of Ports



**Parallel Port**

**Serial Port**

## Serial ports



transmit data one bit at a time, like the picture on the left illustrates.

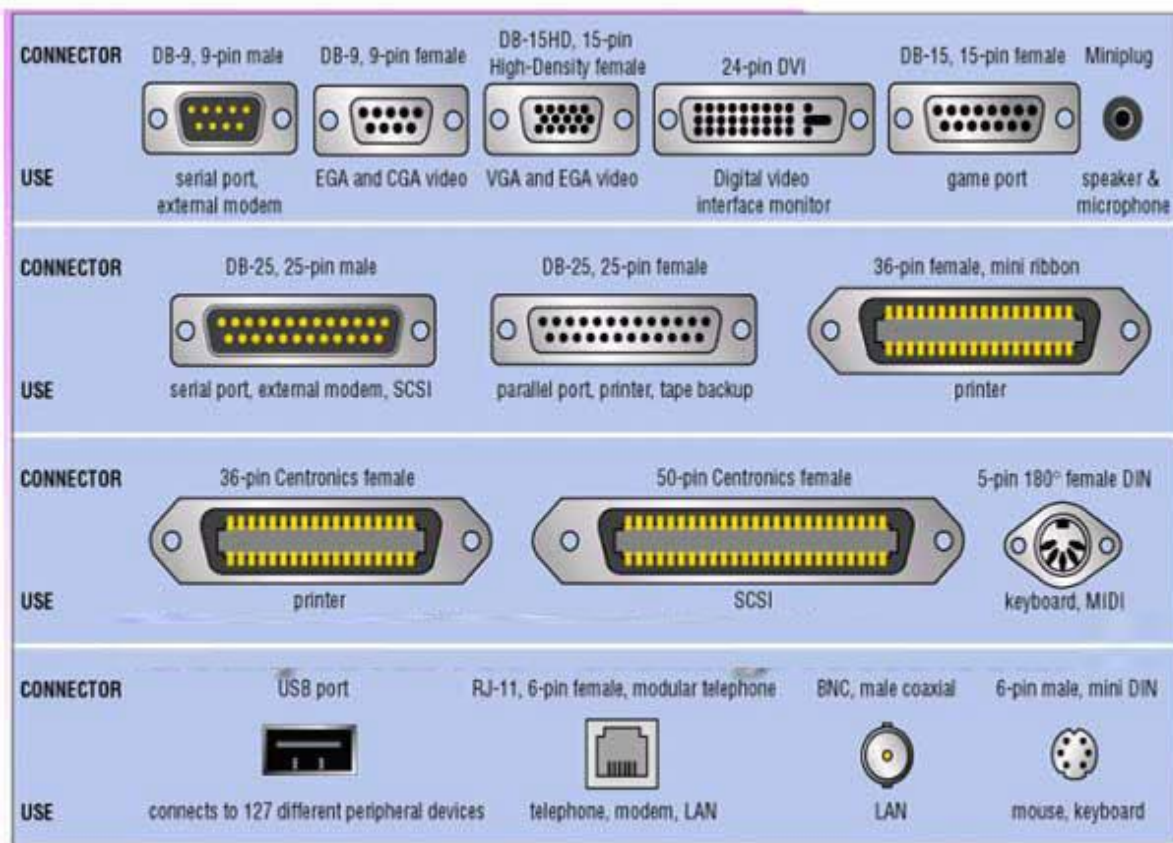
## Parallel ports

transmit more than one byte at a time.

These types of port designs are based on whether or not fast data transmission rates are required by the device or not.

Most computers come with basic types of ports (serial, parallel, keyboard, mouse, and USB); and expansion cards allow you to expand the available types needed by specific devices.

## Different Types of Connectors



Understanding the differences among connector types is useful and important, as the cable required to attach a device to your computer is specific to its connector, not to mention the port on the computer.

## Non-Volatile Storage Devices



## Disk drives

- Internal & External
- Hard drives
- Removable disk drives
- Floppy disks (1.4 MB)
- ZIP disks (100/250 MB)
- CD-ROM (700MB), DVD-ROM (~5GB/side)
- read only (-ROM), write once (-R), re-writeable (-RW)
- Combination drive
- CD-RW/DVD-ROM, CD-RW/DVD-R

Many other forms

Memory Stick, MultiMediaCard, CompactFlash, and SmartMedia