Computer Network
DIT
PART 1ST

Compiled And Arranged By SARDAR AZEEM(PRINCIPAL PICT)

DEFINITION OF COMPUTER NETWORK

A **computer network**, often simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information.

Technically, Network is defined as "If at least one process in one computer is able to send/receive data to/from at least one process residing in a remote computer, then the two computers are said to be in network".

Networks may be classified according to a wide variety of characteristics such as the medium used to transport the data, communications protocol used, scale, topology, and organizational scope.

The rules and data formats for exchanging information in a computer network are defined by communications protocols. Well-known communications protocols are Ethernet, a hardware and Link Layer standard that is ubiquitous in local area networks, and the Internet Protocol Suite, which defines a set of protocols for internetworking, i.e. for data communication between multiple networks, as well as host-to-host data transfer, and application-specific data transmission formats.

HISTORY OF COMPUTER NETWORK;

Before the advent of computer networks that were based upon some type of telecommunications system, communication between calculation machines and early computers was performed by human users by carrying instructions between them. Many of the social behaviors seen in today's Internet were demonstrably present in the 19th century and arguably in even earlier networks using visual signals.

- In September 1940, George Stibitz used a Teletype machine to send instructions for a problem set from his Model at Dartmouth College to his Complex Number Calculator in New York and received results back by the same means. Linking output systems like teletypewriters to computers was an interest at the Advanced Research Projects Agency (ARPA) when, in 1962, J.C.R. Licklider was hired and developed a working group he called the "Intergalactic Network", a precursor to the ARPANET.
- Early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE), started in the late 1950s
- The commercial airline reservation system semi-automatic business research environment (SABRE) which went online with two connected mainframes in 1960.
- In 1964, researchers at Dartmouth developed the Dartmouth Time Sharing System for distributed users of large computer systems. The same year, at Massachusetts Institute of Technology, a research group supported by General Electric and Bell Labs used a computer to route and manage telephone connections.
- Throughout the 1960s Leonard Kleinrock, Paul Baran and Donald Davies independently conceptualized and developed network systems which used packets that could be used in a network between computer systems.
- 1965 Thomas Merrill and Lawrence G. Roberts created the first wide area network (WAN).
- The first widely used telephone switch that used true computer control was introduced by Western Electric in 1965.
- In 1969 the University of California at Los Angeles, the Stanford Research Institute, University of California at Santa Barbara, and the University of Utah were connected as the beginning of the ARPANET network using 50 kbit/s circuits.

- Commercial services using X.25 were deployed in 1972, and later used as an underlying infrastructure for expanding TCP/IP networks.

Today, computer networks are the core of modern communication. All modern aspects of the public switched telephone network (PSTN) are computer-controlled, and telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet.

TYPES OF NETWORK:

Networks are often classified by their physical or organizational extent or their purpose. Usage, trust level, and access rights differ between these types of networks.

Personal area network

A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters. A wired PAN is usually constructed with USB and Firewire connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.

Local area network

A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired LAN using existing home wires (coaxial cables, phone lines and power lines).

Typical library network, in a branching tree topology and controlled access to resources

All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet connection to the central router, could be called "layer 3 switches" because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks' customer access routers.

The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at speeds up to 10 Gbit/s. This is the data transfer rate. IEEE has projects investigating the standardization of 40 and 100 Gbit/s. LANs can be connected to Wide area network by using routers.

Home network

A home network is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or Digital Subscriber Line (DSL) provider.

Storage area network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium sized business environments.

Campus network

A campus network is a computer network made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, **Cat5** cabling etc.) are almost entirely owned (by the campus tenant / owner: an enterprise, university, government etc.).

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including, for example, academic colleges or departments, the university library, and student residence halls.

Backbone network

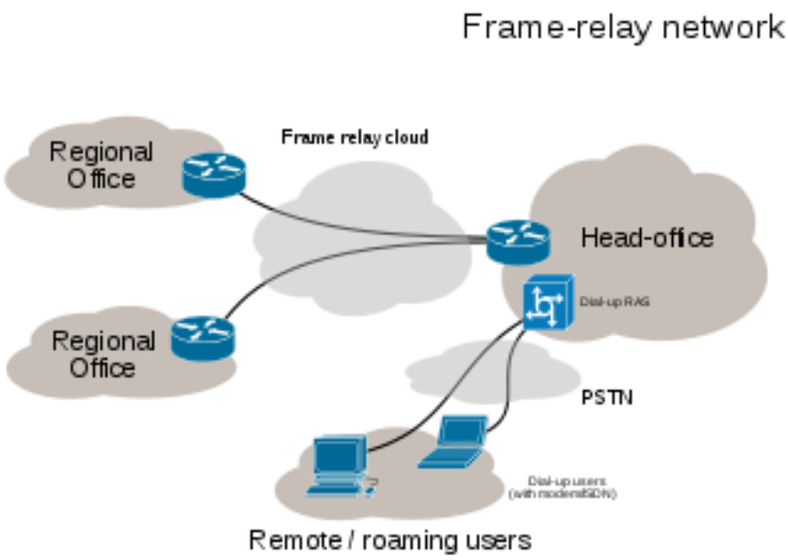
A backbone network is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or subnetworks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than that of the networks connected to it.

A large corporation which has many locations may have a backbone network that ties all of these locations together, for example, if a server cluster needs to be accessed by different departments of a company which are located at different geographical locations. The equipment which ties these departments together constitute the network backbone. Network performance management including network congestion are critical parameters taken into account when designing a network backbone.

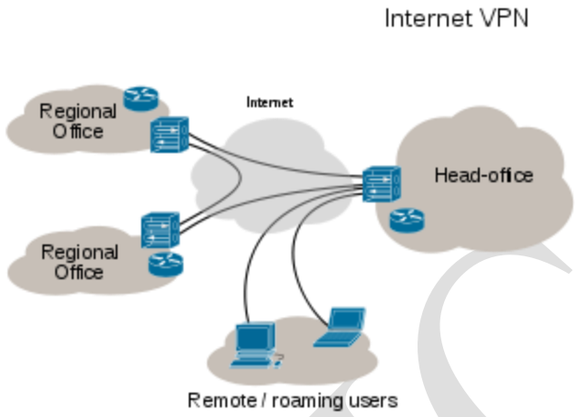
A specific case of a backbone network is the Internet backbone, which is the set of wide-area network connections and core routers that interconnect all networks connected to the Internet.

Metropolitan area network

A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.



Sample EPN made of Frame relay WAN connections and dialup remote access.



Sample VPN used to interconnect 3 offices and remote users

Wide area network

A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

Enterprise private network

An enterprise private network is a network built by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

Virtual private network

A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

Internetwork

An internetwork is the connection of multiple computer networks via a common routing technology using routers. The Internet is an aggregation of many connected internetworks spanning the Earth.

Organizational scope

Networks are typically managed by organizations which own them. According to the owner's point of view, networks are seen as intranets or extranets. A special case of network is the Internet, which has no single owner but a distinct status when seen by an organizational entity – that of permitting virtually unlimited global connectivity for a great multitude of purposes.

Intranets and extranets

Intranets and extranets are parts or extensions of a computer network, usually a LAN.

An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

An extranet is a network that is limited in scope to a single organization or entity and also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities—a company's customers may be given access to some part of its intranet—while at the same time the customers may not be considered *trusted* from a security standpoint. Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

Internet

The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the United States Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW).

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

Basic Network Terminologies:

DATA:

1. Information in raw or unorganized form (such as alphabets, numbers, or symbols) that refer to, or represent, conditions, ideas, or objects. Data is limitless and present everywhere in the universe. See also information and knowledge.

2. Computers: Symbols or signals that are input, stored, and processed by a computer, for output as usable information.

DATA RATE:

Data rate can refer to:

- Bit rate, or data transfer rate
- Data signaling rate
- Data rate units

BIT RATE:

In telecommunications and computing, **bit rate** (sometimes written **bitrate**, **data rate** or as a variable is the number of bits that are conveyed or processed per unit of time.

The bit rate is quantified using the bits per second (**bit/s** or **bps**) unit, often in conjunction with an SI prefix such as kilo- (kbit/s or kbps), mega- (Mbit/s or Mbps), giga- (Gbit/s or Gbps) or tera- (Tbit/s or Tbps). Note that, unlike many other computer-related units, 1 kbit/s is traditionally defined as 1,000-bit/s, not 1,024-bit/s, etc., also before 1999 when SI prefixes were introduced for units of information in the standard IEC 60027-2.

The formal abbreviation for "bits per second" is "bit/s" (not "bits/s", see writing style for SI units). In less formal contexts the abbreviations "b/s" or "bps" are often used, though this risks confusion with "bytes per second" ("B/s", "Bps"). 1 Byte/s (Bps or B/s) corresponds to 8-bit/s (bps or b/s).

DATA SIGNING RATE:

In telecommunication, **data signaling rate** (DSR), also known as gross bit rate, is the aggregate rate at which data pass a point in the transmission path of a data transmission system.

Notes:

1. The DSR is usually expressed in bits per second.
2. The data signaling rate is given by $\sum_{i=1}^{m} \frac{\log_2 n_i}{T_i}$ where m is the number of parallel channels, n_i is the number of significant conditions of the modulation in the i-th channel, and T_i is the unit interval, expressed in seconds, for the i-th channel.
3. For serial transmission in a single channel, the DSR reduces to $(1/T)\log_2 n$; with a two-condition modulation, i. e. $n = 2$, the DSR is $1/T$, according to Hartley's law.
4. For parallel transmission with equal unit intervals and equal numbers of significant conditions on each channel, the DSR is $(m/T)\log_2 n$; in the case of a two-condition modulation, this reduces to m/T.
5. The DSR may be expressed in bauds, in which case, the factor $\log_2 n_i$ in the above summation formula should be deleted when calculating bauds.
6. In synchronous binary signaling, the DSR in bits per second may be numerically the same as the modulation rate expressed in bauds. Signal processors, such as four-phase modems, cannot change the DSR, but the modulation rate depends on the line modulation scheme, in accordance with Note 4. For example, in a 2400 bit/s 4-phase sending modem, the signaling rate is 2400 bit/s on the serial input side, but the modulation rate is only 1200 bauds on the 4-phase output side.

DATA RATE UNITS;

n telecommunications, bit rate or data transfer rate is the average number of bits, characters, or blocks per unit time passing between equipment in a data transmission system. This is typically measured in multiples of the unit *bit per second* or *byte per second*.

Bit rates		
Decimal prefixes (SI)		
Name	**Symbol**	**Multiple**
kilobit per second	kbit/s	10^3
megabit per second	Mbit/s	10^6
gigabit per second	Gbit/s	10^9
terabit per second	Tbit/s	10^{12}
Binary prefixes (IEC 60027-2)		
kibibit per second	Kibit/s	2^{10}
mebibit per second	Mibit/s	2^{20}
gibibit per second	Gibit/s	2^{30}
tebibit per second	Tibit/s	2^{40}

To be as explicit as possible, both the prefix and the suffix of the unit must be known. For example, the abbreviation *2 Mb* can actually be expanded in 2 different ways (*mega-* vs *mebi-* and *-bit* vs *-byte*). The difference in the associated numbers can be significant:

Unit	Bits	Bits / 1,000,000
Mega-bit	1,000,000	1.0
Mebi-bit	1,048,576	1.05
Mega-byte	8,000,000	8.0
Mebi-byte	8,388,608	8.39

The table above shows an approximate 5% difference between the corresponding mega- and mebi- units with a 800% difference between -bit and -byte units. Explicitness in units is important because difference can become even larger across different prefix units).

Prefix: *k* vs *Ki*

k- stands for kilo, meaning 1,000, while *Ki-* stands for *kilobinary* ("kibi-"), meaning 1,024. The standardized binary prefixes such as *Ki-* were relatively recently introduced and still face low adoption. *K-* is often used to mean 1,024, especially in *KB*, the kilobyte.

Suffix: *b* vs *B*

b stands for *bit* and *B* stands for *byte*. In the context of data rate units, one byte refers to 8 bits. For example, when a *1 Mbps* connection is advertised, it usually means that the maximum achievable download bandwidth is 1 megabit/s (million bits per second), which is actually 0.125 MB/s (megabyte per second), or about 0.1192 MiB/s (mebibyte per second).

Problems

In 1999, the International Electrotechnical Commission (IEC) published Amendment 2 to "IEC 60027-2: Letter symbols to be used in electrical technology – Part 2: Telecommunications and electronics." This standard, approved in 1998, introduced the prefixes kibi-, mebi-, gibi-, tebi-, pebi-, and exbi- to be used in specifying binary multiples of a quantity. The name is derived from the first two letters of the original SI prefixes followed by bi (short for *binary*). It also clarifies that the SI prefixes be used only to mean powers of 10 and never powers of 2.

The correct use for file, disk, and memory size is as follows:

Unit (SI)	Bytes	Unit (IEC 60027-2)	Bytes
Kilobyte (kB)	1,000	Kibibyte (KiB)	1,024
Megabyte (MB)	$1{,}000^2$	Mebibyte (MiB)	$1{,}024^2$
Gigabyte (GB)	$1{,}000^3$	Gibibyte (GiB)	$1{,}024^3$
Terabyte (TB)	$1{,}000^4$	Tebibyte (TiB)	$1{,}024^4$
Petabyte (PB)	$1{,}000^5$	Pebibyte (PiB)	$1{,}024^5$

Computer and technology industries have yet to adapt to these standards. When Microsoft Windows shows the size of a drive or a file, it uses powers of 1,024 but uses SI prefixes so that, for example, 28,735,078,400 bytes displays as *26.7 GB* instead of either 28.7 GB, or 26.7 GiB.

The commonly advertised (formatted) capacity of the 3.5-inch floppy disk was 1.44 MB but was actually 1,440 KiB or 1.44 × 1,000 × 1,024 bytes, giving either 1.41 MiB or 1.47 MB.

On September 18, 2003, Reuters reported that Apple, Dell, Gateway, Hewlett-Packard, IBM, Sharp, Sony, and Toshiba were being sued in a class-action law-suit in the Los Angeles Superior Court for "deceiving" buyers as to the true capacity of those companies' hard drives. This of course was due to ambiguity of *GB* when used by software and hardware vendors.

Decimal multiples of bits

Kilobit per second

A **kilobit per second** (**kbit/s**, **kb/s**, or **kbps**) is a unit of data transfer rate equal to:

- 1000 bits per second or
- 125 bytes per second.

Megabit per second

A **megabit per second** (**Mbit/s**, **Mb/s**, or **Mbps**; not to be confused with **mbit/s** which means, literally, ***milli*bit per second**) is a unit of data transfer rate equal to:

- 1,000,000 bits per second or
- 1,000 kilobits per second or
- 125,000 bytes per second.

Gigabit per second

A **gigabit per second** (**Gbit/s**, **Gb/s**, or **Gbps**) is a unit of data transfer rate equal to:

- 1,000 megabits per second or
- 1,000,000 kilobits per second or
- 1,000,000,000 bits per second or
- 125,000,000 bytes per second

Binary multiples of bits

Kibibit per second

A **kibibit per second** (**Kibit/s** or **Kib/s**) is a unit of data transfer rate equal to 1,024 bits per second. The word "kibibit" is not capitalized, but the abbreviation "Kibits" is.

Mebibit per second

A **mebibit per second** (**Mibit/s** or **Mib/s**) is a unit of data transfer rate equal to:

- 1,048,576 bits per second or
- 1,024 kibibits per second.

Gibibit per second

A **gibibit per second** (**Gibit/s** or **Gib/s**) is a unit of data transfer rate equal to:

- 1,073,741,824 bits per second or
- 1,048,576 kibibits per second or
- 1,024 mebibits per second.

Tebibit per second

A **tebibit per second** (**Tibit/s** or **Tib/s**) is a unit of data transfer rate equal to:

- 1,099,511,627,776 bits per second or
- 1,073,741,824 kibibits per second or
- 1,048,576 mebibits per second or
- 1,024 gibibits per second.

Decimal multiples of bytes

WARNING: These units are often not used in the suggested ways! See section above, "Problems".

Kilobyte per second

A **kilobyte per second** is a unit of data transfer rate equal to:

- 8,000 bits per second, or
- 1,000 bytes per second, or
- 8 kilobits per second.

Megabyte per second

(not to be confused with Mbps - Mega bits per second) A **megabyte per second** (**MB/s** or **MBps**) is a unit of data transfer rate equal to:

- 8,000,000 bits per second, or
- 1,000,000 bytes per second, or
- 1,000 kilobytes per second, or
- 8 megabits per second.

Gigabyte per second

A **gigabyte per second** (**GB/s** or **GBps**) is a unit of data transfer rate equal to:

- 8,000,000,000 bits per second, or
- 1,000,000,000 bytes per second, or
- 1,000,000 kilobytes per second, or
- 1,000 megabytes per second, or
- 8 gigabits per second.

Terabyte per second

A **terabyte per second** (**TB/s** or **TBps**) is a unit of data transfer rate equal to:

- 8,000,000,000,000 bits per second, or
- 1,000,000,000,000 bytes per second, or
- 1,000,000,000 kilobytes per second, or
- 1,000,000 megabytes per second, or
- 1,000 gigabytes per second, or
- 8 terabits per second.

Binary multiples of bytes

Kibibyte per second

A **kibibyte per second** (**KiB/s** or **KiBps**) is a unit of data transfer rate equal to:

- 1,024 bytes per second, or
- 8 kibibits per second, or
- 8192 bits per second.

Mebibyte per second

A **mebibyte per second** (**MiB/s** or **MiBps**) is a unit of data transfer rate equal to:

- 1,048,576 bytes per second, or
- 1,024 kibibytes per second, or
- 8 mebibits per second, or
- 8192 kibibits per second, or
- 8,388,608 bits per second.

Gibibyte per second

A **gibibyte per second** (**GiB/s** or **GiBps**) is a unit of data transfer rate equal to:

- 1,073,741,824 bytes per second, or
- 1,048,576 kibibytes per second, or
- 1,024 mebibytes per second, or
- 8 gibibits per second, or
- 8192 mebibits per second, or
- 8,388,608 kibibits per second, or
- 8,589,934,592 bits per second.

Tebibyte per second

A **tebibyte per second** (**TiB/s** or **TiBps**) is a unit of data transfer rate equal to:

- 1,099,511,627,776 bytes per second, or
- 1,073,741,824 kibibytes per second, or
- 1,048,576 mebibytes per second, or
- 1,024 gibibytes per second, or
- 8 tebibits per second.
- 8192 gibibits per second, or
- 8,388,608 mebibits per second, or
- 8,589,934,592 kibibits per second, or
- 8,796,093,022,208 bits per second.

BAUD RATE:

In digital communications, **symbol rate** (also known as baud or modulation rate) is the number of symbol changes (waveform changes or signalling events) made to the transmission medium per second using a digitally modulated signal or a line code. The Symbol rate is measured in baud (Bd) or symbols/second. In the case of a line code, the symbol rate is the pulse rate in pulses/second. Each symbol can represent or convey one or several bits of data. The symbol rate is related to, but should not be confused with, the gross bitrate expressed in bit/second.

PEAK DATA RATE:

The maximum data rate of the traffic.

BURSITY DATA:

In telecommunication, the term **burst transmission** or **data burst** has the following meanings:

1. Any relatively high-bandwidth transmission over a short period of time. For example, a download might use 2 Mbit/s on average, while having "peaks" bursting up to, say, 2.4 Mbit/s.
2. Transmission that combines a very high data signaling rate with very short transmission times - i.e., the message is compressed. This is popular with the military and spies, who both wish to minimize the chance of their radio transmissions being detected, i.e. Low probability of intercept (LPI) and Low probability of recognition (LPR).
3. Operation of a data network in which data transmission is interrupted at intervals.

PEER TO PEER NETWORK VS SERVER BASED NETWORK

Peer-to-peer

A network is either a peer-to-peer network (also called a workgroup) or a server-based network (also called a client/server network).

Peer-to-peer network

In a peer-to-peer network a group of computers is connected together so that users can share resources and information. There is no central location for authenticating users, storing files, or accessing resources. This means that users must remember which computers in the workgroup have the shared resource or information that they want to access. It also means that users must log on to each computer to access the shared resources on that computer.

In most peer-to-peer networks, it is difficult for users to track where information is located because data is generally stored on multiple computers. This makes it difficult to back up critical business information, and it often results in small businesses not completing backups. Often, there are multiple versions of the same file on different computers in the workgroup.

In some peer-to-peer networks, the small business uses one computer that is running a client operating system, such as Microsoft Windows 98 or Windows XP Professional, as the designated "server" for the network. Although this helps with saving data in a central location, it does not provide a robust solution for many of the needs of a small business, such as collaborating on documents.

Server-based network

In a server-based network, the server is the central location where users share and access network resources (see Figure 4). This dedicated computer controls the level of access that users have to shared resources. Shared data is in one location, making it easy to back up critical business information. Each computer that connects to the network is called a client computer. In a server-based network, users have one user account and password to log on to the server and to access shared resources. Server operating systems are designed to handle the load when multiple client computers access server-based resources.

Windows SBS 2008 is installed and configured as the central server on a server-based network. Windows SBS 2008 provides the central point for authenticating users, accessing resources, and storing information.

What is a Topology?

The physical layout of a network is called network topology. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Logical topology was discussed in the Protocol chapter.

Main Types of Physical Topologies

The following sections discuss the physical topologies used in networks and other related topics.

- Linear Bus
- Star
- Tree (Expanded Star)
- Ring topology
- Mesh Topology
- Hybrid Topology

Linear Bus

A linear bus topology consists of a main run of cable with a terminator at each end. All nodes (file server, workstations, and peripherals) are connected to the linear cable.

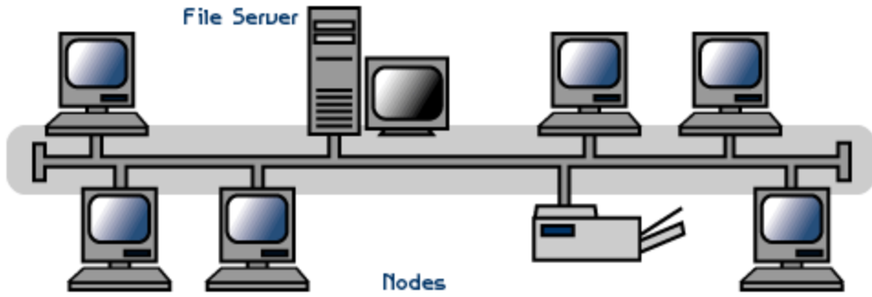


Fig. 1. Linear Bus topology

Advantages of a Linear Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of a Linear Bus Topology

- Entire network shuts down if there is a break in the main cable.

- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution in a large building.

Star

A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator (See fig. 2).

Data on a star network passes through the hub, switch, or concentrator before continuing to its destination. The hub, switch, or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

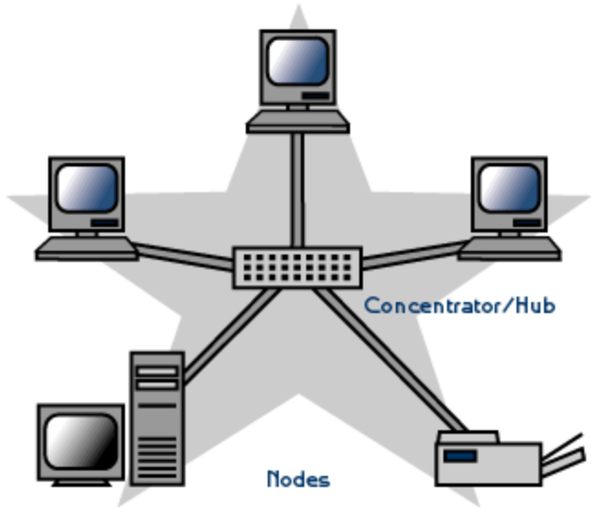


Fig. 2. Star topology

Advantages of a Star Topology

- Easy to install and wire.
- No disruptions to the network when connecting or removing devices.
- Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

- Requires more cable length than a linear topology.
- If the hub, switch, or concentrator fails, nodes attached are disabled.
- More expensive than linear bus topologies because of the cost of the hubs, etc.

Tree or Expanded Star

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable (See fig. 3). Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

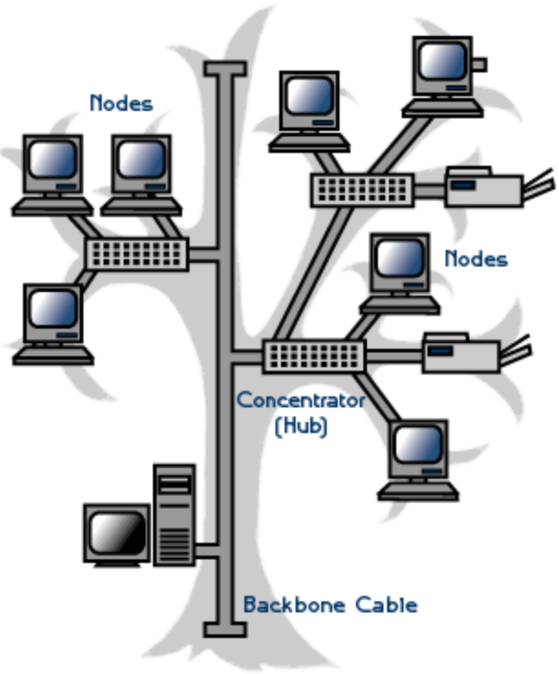


Fig. 3. Tree topology

Advantages of a Tree Topology

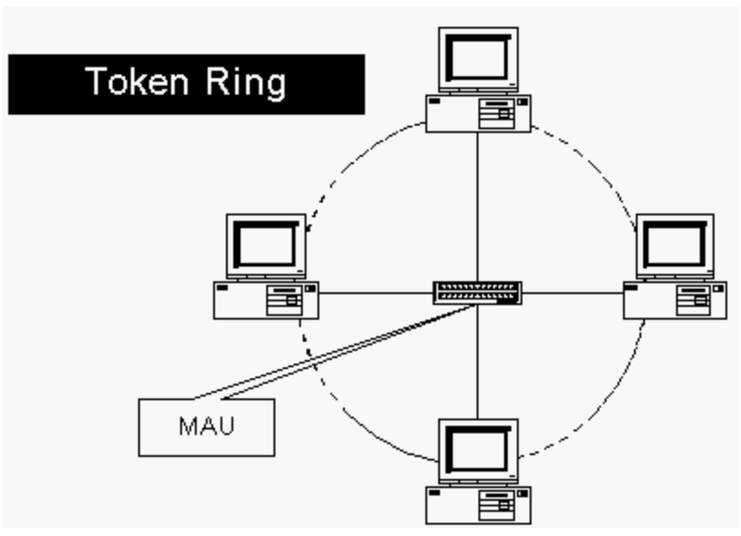
- Point-to-point wiring for individual segments.
- Supported by several hardware and software venders.

Disadvantages of a Tree Topology

- Overall length of each segment is limited by the type of cabling used.
- If the backbone line breaks, the entire segment goes down.
- More difficult to configure and wire than other topologies.

Ring topology?

A ***ring topology*** consists of a set of stations connected serially by cable. In other words, it's a circle or ring of computers. There are no terminated ends to the cable; the signal travels around the circle in a clockwise direction.



Note that while this topology functions logically as ring, it is physically wired as a star. The central connector is not called a hub but a ***Multistation Access Unit*** or ***MAU***. (Don't confuse a Token Ring MAU with a 'Media Adapter Unit' which is actually a transceiver.)

Under the ring concept, a signal is transferred sequentially via a "token" from one station to the next. When a station wants to transmit, it "grabs" the token, attaches data and an address to it, and then sends it around the ring. The token travels along the ring until it reaches the destination address. The receiving computer acknowledges receipt with a return message to the sender. The sender then releases the token for use by another computer.

Each station on the ring has equal access but only one station can talk at a time.

In contrast to the 'passive' topology of the bus, the ring employs an '***active'*** topology. Each station repeats or 'boosts' the signal before passing it on to the next station.

Rings are normally implemented using twisted pair or fiber-optic cable.

▲8. What are the advantages and disadvantages of a ring topology?

Advantages of ring topology:

- Growth of system has minimal impact on performance
- All stations have equal access

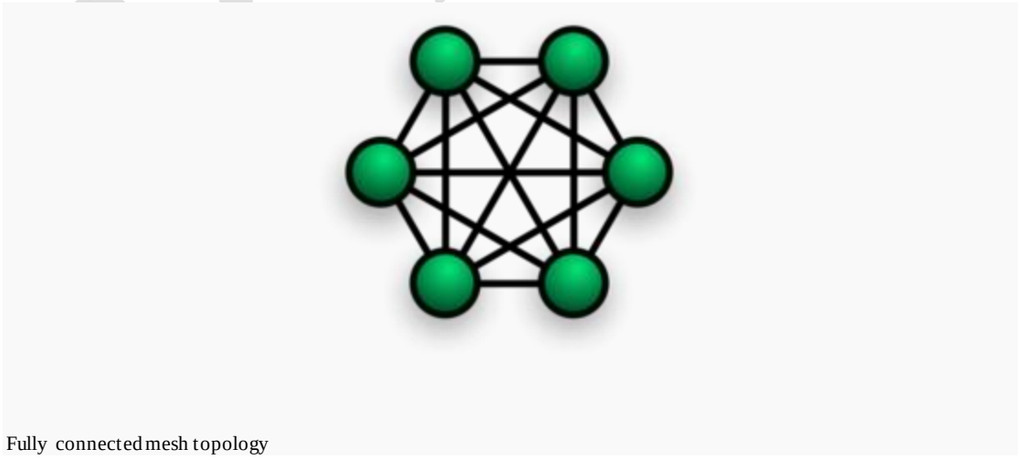
Disadvantages of ring topology:

- Most expensive topology
- Failure of one computer may impact others
- Complex

MESH TOPOLOGY:

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

Fully connected

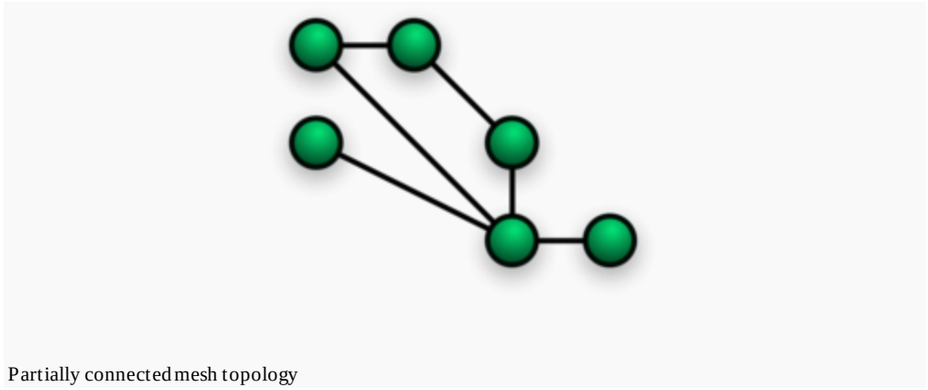


Fully connected mesh topology

The number of connections in a full mesh = n(n - 1) / 2.

Note: The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected (see Combinatorial explosion).

Partially connected



Partially connected mesh topology

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

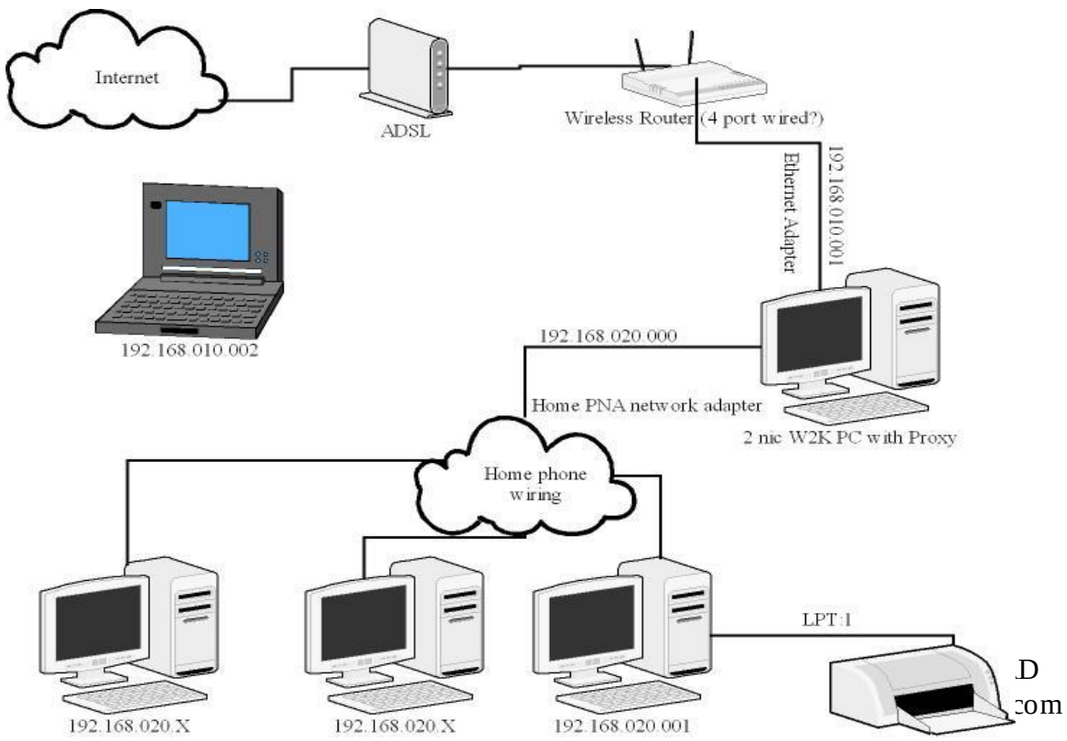
Note: In most practical networks that are based upon the partially connected mesh topology, all of the data that is transmitted between nodes in the network takes the shortest path between nodes,[*citation needed*] except in the case of a failure or break in one of the links, in which case the data takes an alternative path to the destination. This requires that the nodes of the network possess some type of logical 'routing' algorithm to determine the correct path to use at any particular time.

Hybrid Network Topology

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

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

While grid and torus networks have found popularity in high-performance computing applications, some systems have used genetic algorithms to design custom networks that have the fewest possible hops in between different nodes. Some of the



resulting layouts are nearly incomprehensible, although they function quite well.[citation needed]

A Snowflake topology is really a "Star of Stars" network, so it exhibits characteristics of a hybrid network topology but is not composed of two different basic network topologies being connected together. Definition : Hybrid topology is a combination of Bus ,Star and ring topology.

Networking Devices

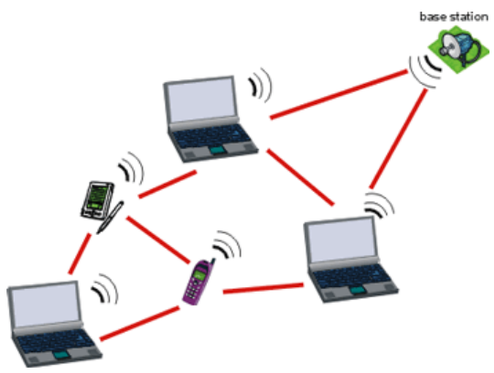
Computer network devices also known as communication devices and they constitute a data communication network. These devices are routers, switches, hubs, LAN cards, gateway, modems, hardware firewall, CSU/DSU, ISDN terminals and transceivers. In an Ethernet or WAN network, the data communication cannot be performed without these devices. Being an IT professional or a network administrator, you must have the good understanding of these devices.

Based on your business requirements, you have the select the best devices for your network and before selection, make sure that they are compatible with each other. It is recommended that you select all the devices for your IT infrastructure from the same vendor.

1. Node
2. Routers
3. Switches
4. Hubs
5. Modems
6. LAN Cards
7. Multiplexer
8. Bridge
9. NIC Card
10. Repeater
11. B-router
12. Gateways

1. Node

In communication networks, a **node** (Latin *nodus*, 'knot') is a connection point, either a redistribution point or a communication endpoint (some terminal equipment). The definition of a node depends on the network and protocol layer referred to. A physical network node is an active electronic device that is attached to a network, and is capable of sending, receiving, or forwarding information over a communications channel.



a. Computer network nodes

In data communication, a physical network node may either be a data circuit-terminating equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment (DTE) such as a digital telephone handset, a printer or a host computer, for example a router, a workstation or a server.

If the network in question is a LAN or WAN, every LAN or WAN node (that are at least data link layer devices) must have a MAC address, typically one for each network interface controller it possesses. Examples are computers, packet switches, xDSL modems (with Ethernet interface) and wireless LAN access points. Note that a hub constitutes a physical network node, but does not constitute a LAN network node, since a hubbed network logically is a bus network. Analogously, a repeater or PSTN modem (with serial interface) is a physical network node but not a LAN node in this sense.

b. Telecommunication network nodes

In the fixed telephone network, a node may be a public or private telephone exchange, a remote concentrator or a computer providing some intelligent network service. In cellular communication, switching points and databases such as the Base station controller, Home Location Register, Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN) are examples of nodes. Cellular network base stations are not considered as nodes in this context.

In cable television systems (CATV), this term has assumed a broader context and is generally associated with a fiber optic node. This can be defined as those homes or businesses within a specific geographic area that are served from a common fiber optic receiver. A fiber optic node is generally described in terms of the number of "homes passed" that are served by that specific fiber node.

c. Distributed system nodes

If the network in question is a distributed system, the nodes are clients, servers or peers. A peer may sometimes serve as client, sometimes server. In a **peer-to-peer** or overlay network, nodes that actively route data for the other networked devices as well as themselves are called supernodes.

2. Routers

A router is a communication device that is used to connect two logically and physically different networks, two LANs, two WANs and a LAN with WAN. The main function of the router is to sorting and the distribution of the data packets to their destinations based on their IP addresses. Routers provides the connectivity between the enterprise businesses, ISPs and in the internet infrastructure, router is a main device. Cisco routers are widely used in the world. Every router has routing software, which is known as IOS. Router operates at the network layer of the OSI model. Router does not broadcast the data packets.

3. Switches

Like the router, a switch is an intelligent device that maps the IP address with the MAC address of the LAN card. Unlike the hubs, a switch does not broadcast the data to all the computers, it sends the data packets only to the destined computer. Switches are used in the

LAN, MAN and WAN. In an Ethernet network, computers are directly connected with the switch via twisted pair cables. In a network, switches use the three methods to transmit the data i.e. store and forward, cut through and fragment free.

A switch comes in different ports like 6, 8, 16, 24 and uplink ports, which are used to connect to other switches in the network. Switch is very important device in the WAN communications too.

Advance switches are used in the telecommunication networks, ISPs and corporate networks. A LAN or WAN switch routes the data packets based on the MAC and IP address of the data. There are different vendors of the switches and Cisco is the biggest manufacturer and provider of the routers and switches. Other manufacturers include Juniper, Jupiter, D-Link, Linksys and Baynet etc.
To make a switched network make sure that all the switches and other network communication devices are compatible with each other.

4. Hubs

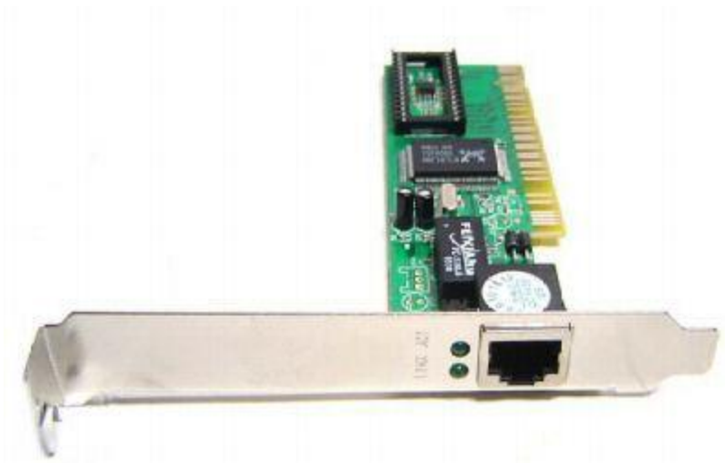
The central connecting device in a computer network is known as a hub. There are two types of a hub i.e. active hub and passive hub. Every computer is directly connected with the hub. When data packets arrives at hub, it broadcast them to all the LAN cards in a network and the destined recipient picks them and all other computers discard the data packets. Hub has five, eight, sixteen and more ports and one port is known as uplink port, which is used to connect with the next hub.

5. Modems

A modem is a communication device that is used to provide the connectivity with the internet. Modem works in two ways i.e. modulation and demodulation. It coverts the digital data into the analog and analog to digital.

6. LAN Cards

LAN cards or network adapters are the building blocks of a computer network. No computer can communicate without a properly installed and configured LAN card. Every LAN card is provided with a unique IP address, subnet mask, gateway and DNS (if applicable). An UTP/STP cable connects a computer with the hub or switch. Both ends of the cable have the RJ-45 connectors one is inserted into the LAN card and one in the hub/switch. LAN cards are inserted into the expansion slots inside the computer. Different LAN cards support different speed from 10/100 to 10/1000.



7. Multiplexer

Multiplexer is a device that is used to combining the several electrical signals into one signal.

8. Bridge

A bridge is a network communication device that is used to connect one segment of the network with another that uses the same protocol. It operates at the Data link layer of the OSI layers model. In the Ethernet network, the bridge is also known as IEEE 802.1D. A bridge process the information at the data link layer of the OSI layers model. There are two types of the bridging.

- Transparent bridging
- Source route bridging

The main advantages of the bridges include the following.

- Inexpensive
- Self Configuring
- Reduced size of the collision domains.
- Transmits the data based on the MAC address.
- Supports relatively big networks.

Bridges are fast devices for forwarding the data but not as fast as the routers and switches. A bridge cannot be used as a firewall device as a router. In the bridged network, the messages are sent to all the nodes and are picked up only by the destined computers. A bridged when combined with the router, known as a brouter. Bridges has now replaced the switches and routers.

9. NIC Card

NIC Stands for Network Interface card. It is one of the most important computer network devices that are used for the data communication and to connect the computers with each other. It is plugged inside the computer either in the PCI slot or it is built-in the motherboard.

A twisted pair UTP/STP with RJ45 connector is used to connect the computer with the Hub or Switch. Fiber optic cable can also be used to connect the computer with the hub or switch.

A NIC can be wired or wireless and it has digital circuitry and microprocessor. A wireless NIC is used to connect the computers with each other wirelessly. There are different vendors of the NIC such as D-Link, 3Com, Intel, Realtek, Baylan and Baynet.

Before buying and installing a network interface card in your computer make sure that it is compatible with the other network devices. NIC card operates on the Data Link and physical layer of the OSI layers model.
For every computer in a network, it is required to have a NIC to communicate with other computers.

Every NIC has unique MAC address and no two NIC cards from two different vendors can have the same MAC address. NIC has twisted pair, BNC and AUI sockets. The one end of the network cable is used to connect with the NIC and the other end is used to connect with the hub or switch.

NIC provides the fulltime connectivity for the data transmission. Sometimes computers do not communicate with each other due to the malfunctioning of the NIC. The network interface cards problems can be resolved with the following tips.

- Make sure that you have the updated and correct version of the LAN card's driver.
- Ensure that the LEDs of the NIC are working properly.
- Check that the network cable is properly connected at both ends.

- Right click on the network status icon on the right bottom of the desktop and click repair.
- Ensure that the TCP/IP settings are accurate.
- Disable the antivirus and firewall.
- If the problem still persists then try to replace the NIC with a new one.

Hub or a switch in a computer network acts as a relay that passes the information from one computer to another. It is important that the LAN card is compatible with the hub or switch to make the data flow faster to avoid the packet loss and network congestion.

10. Repeater

repeater is a communication device that retransmits the weak signals with greater power. It receives the signals over the wireless, optical transmission and network cable mediums such as copper wire, UTP/STP and fiber optic cables and regenerates the analog or digital signals. It can relay the data signals between the different subnetworks.

Repeater operates at the physical layer of the OSI layers model and it is not such as intelligent device like the switches and routers that perform the smart routing based on the MAC and IP addresses of the source and destination computers. Repeaters are also used in the broadcasting, where they are known as the relay transmitters and boosters. Repeaters restrengthen the data signals in the telecommunications. Normally a repeater consists of the following things.

- Amplifier
- Transmitter
- Isolator
- Antennas
- Radio Receiver

In a fiber optic network, a repeater consists of the following.

- Amplifier
- Photocell
- IRED
- IR
- LED

Fiber optic repeaters are less expensive and operate at low power. Repeaters were also used to connect the segments of the cables. Repeaters are of mainly two types i.e. with internal antenna and with external antenna. If you are using repeater in your network make sure that is it compatible with other devices in your network.

11. B-router

Bridge Router

A **Bridge Router** or **router** is a network device that works as a bridge and as a router. The brouter routes packets for known protocols and simply forwards all other packets as a bridge would.

Brouters operate at both the network layer for routable protocols and at the data link layer for non-routable protocols. As networks continue to become more complex, a mix of routable and non-routable protocols has led to the need for the combined features of bridges and routers. Brouters handle both routable and non-routable features by acting as routers for routable protocols and bridges for non-routable protocols. Bridged protocols might propagate throughout the network, but techniques such as filtering and learning might be used to reduce potential congestion. Brouters are used as connecting devices in the networking system, so it acts as a bridge in a network and as a router in an internetwork.

12. Gateways

In telecommunications, the term **gateway** has the following meaning:

1. In a communications network, a network node equipped for interfacing with another network that uses different protocols.
    a. A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.
    b. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.
2. Loosely, a computer or computer program configured to perform the tasks of a gateway.

Gateways, also called protocol converters, can operate at any network layer. The activities of a gateway are more complex than that of the router or switch as it communicates using more than one protocol.

Transmission media

Network Media Types

is the actual path over which an electrical signal travels as it moves from one component to another. including twisted-pair cable, coaxial cable, fiber-optic cable, and wireless.

There are two main types of network media

1. Guided /Wired Media:

A network media that consists of physical cables

Eg coaxial cable
Twisted pair cable
Fiber optic cable

2. Unguided media

Does not consist of physical cables

Eg radio waves
Micro waves
Satellite Waves
Infrared

Twisted-Pair Cable

Is a type of cabling that is used for telephone communications and most Modern Ethernet networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against *crosstalk* the noise generated by adjacent pairs.

When electrical current flows through a wire, it creates a small, circular magnetic field around the wire. When two wires in an electrical circuit are placed close together, their magnetic fields are the exact opposite of each other. Thus, the two magnetic fields cancel each other out. They also cancel out any outside magnetic fields. Twisting the wires can enhance this *cancellation effect*.

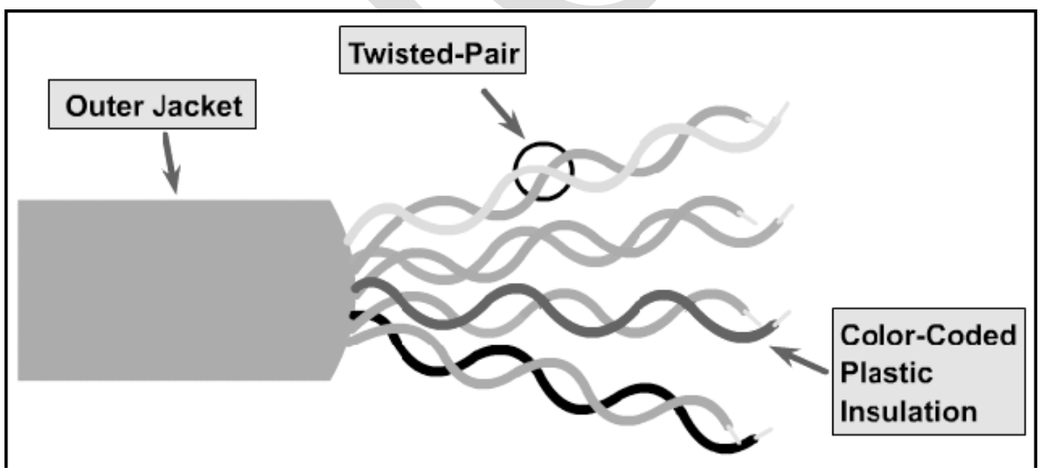
Using cancellation together with twisting the wires, cable designers can effectively provide self-shielding for wire pairs within the network media.

Two basic types of twisted-pair cable exist: unshielded twisted pair (UTP) and shielded twisted pair (STP). The following sections discuss UTP and STP cable in more detail.

UTP Cable

UTP cable is a medium that is composed of pairs of wires (see Figure 8-1).

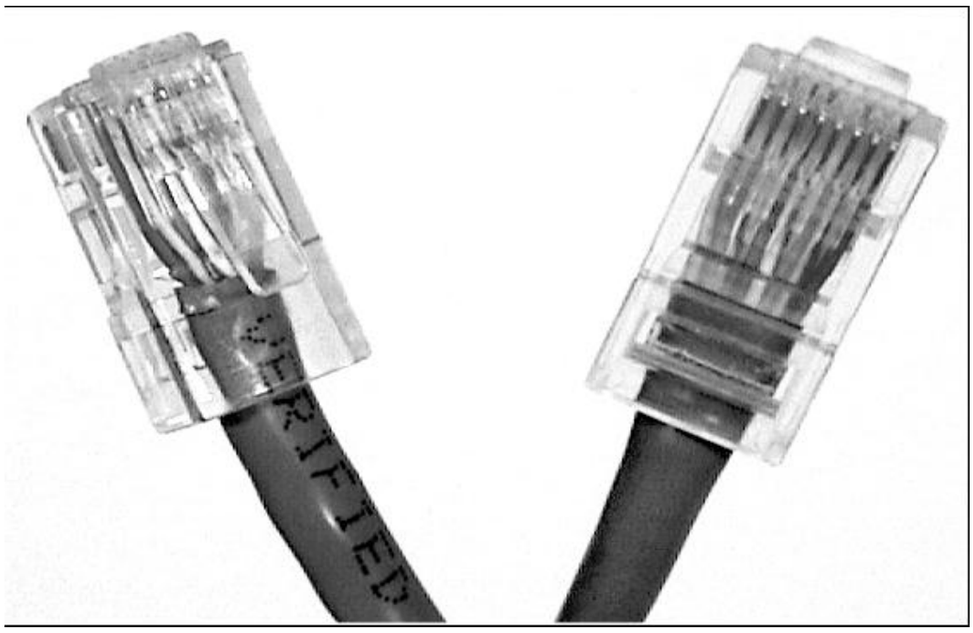
UTP cable is used in a variety of networks. Each of the eight individual copper wires in UTP cable is covered by an insulating material. In addition, the wires in each pair are twisted around each other.



UTP cable relies solely on the cancellation effect produced by the twisted wire pairs to limit signal degradation caused by electromagnetic interference (EMI) and radio frequency interference (RFI). To further reduce crosstalk between the pairs in UTP cable, the number of twists in the wire pairs varies. UTP cable must follow precise specifications governing how many twists or braids are permitted per meter (3.28 feet) of cable.

UTP cable often is installed using a Registered Jack 45 (RJ-45) connector .

The RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area network (LAN), especially Ethernets.



When used as a networking medium, UTP cable has four pairs of either 22- or 24-gauge copper wire. UTP used as a networking medium has an impedance of 100 ohms; this differentiates it from other types of twisted-pair wiring such as that used for telephone wiring, which has impedance of 600 ohms.

UTP cable offers many advantages. Because UTP has an external diameter of approximately 0.43 cm (0.17 inches), its small size can be advantageous during installation. Because it has such a small external diameter, UTP does not fill up wiring ducts as rapidly as other types of cable. This can be an extremely important factor to consider, particularly when installing a network in an older building. UTP cable is easy to install and is less expensive than other types of networking media. In fact, UTP costs less per meter than any other type of LAN cabling. And because UTP can be used with most of the major networking architectures, it continues to grow in popularity.

Disadvantages also are involved in using twisted-pair cabling, however. UTP cable is more prone to electrical noise and interference than other types of networking media, and the distance between signal boosts is shorter for UTP than it is for coaxial and fiber-optic cables.

Although UTP was once considered to be slower at transmitting data than other types of cable, this is no longer true. In fact, UTP is considered the fastest copper-based medium today. The following summarizes the features of UTP cable:

• **Speed and throughput**
—10 to 1000 Mbps
• **Average cost per node**
—Least expensive
• **Media and connector size**
—Small
• **Maximum cable length**
—100 m (short) Commonly used types of UTP cabling are as follows:

Category 1
—Used for telephone communications. Not suitable for transmitting data.

Category 2
—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).

Category 3
—Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.

Category 4
—Used in Token Ring networks. Can transmit data at speeds up to 16 Mbps.

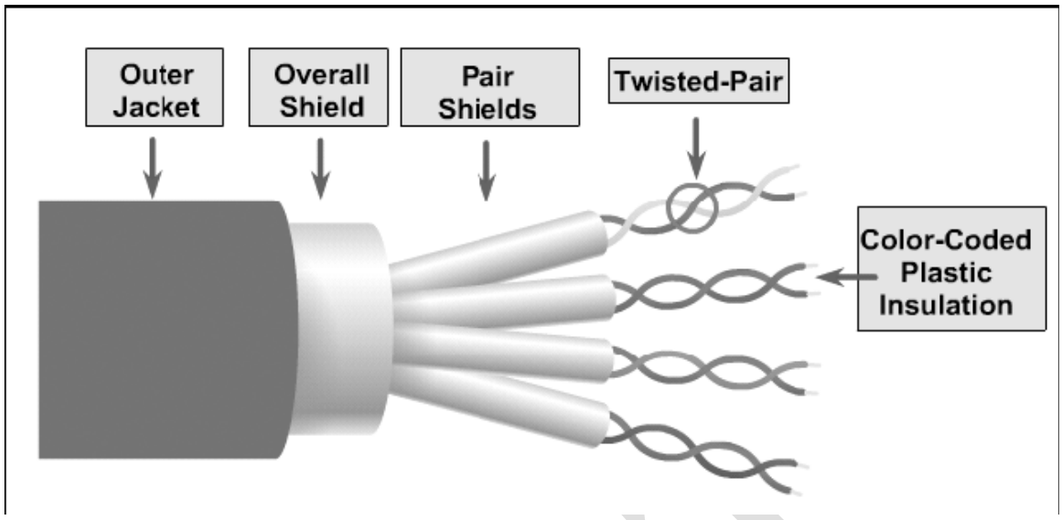
Category 5
—Can transmit data at speeds up to 100 Mbps.

Category 5e
—Used in networks running at speeds up to 1000 Mbps (1 gigabit per second Gbps]).

Category 6
—Typically, Category 6 cable consists of four pairs of 24 American Wire Gauge (AWG) copper wires. Category 6 cables are currently the fastest standard for UTP.

Shielded Twisted-Pair Cable

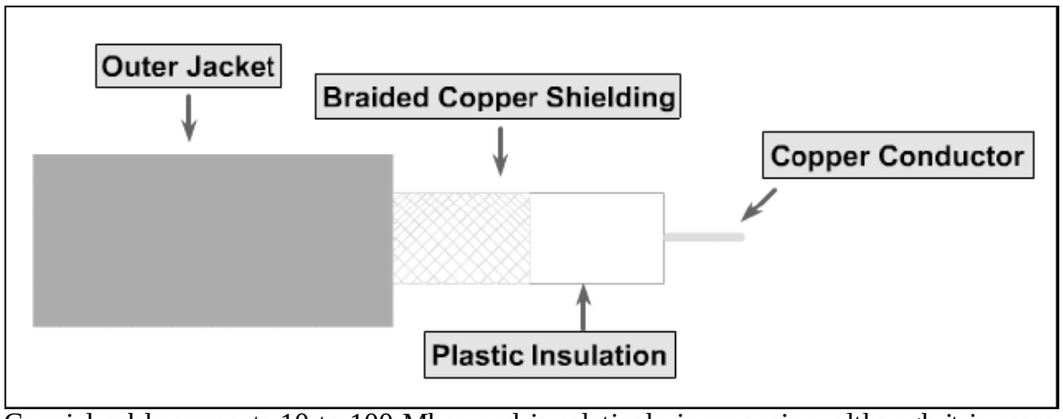
Cable combines the techniques of shielding, cancellation, and wire
Twisting. Each pair of wires is wrapped in a metallic foil (see Figure 8-3). The four pairs of wires then are wrapped in an overall metallic braid or foil, usually 150-ohm cable. As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable (pairto- pair coupling, or crosstalk) and from outside the cable (EMI and RFI). STP usually is installed with STP data connector, which is created especially for the STP cable. However, STP cabling also can use the same RJ connectors that UTP uses.



Although STP prevents interference better than UTP, it is more expensive and difficult to install.
In addition, the metallic shielding must be grounded at both ends. If it is improperly grounded, the shield acts like an antenna and picks up unwanted signals. Because of its cost and difficulty with termination, STP is rarely used in Ethernet networks. STP is primarily used in Europe.
The following summarizes the features of STP cable:
Speed and throughput
—10 to 100 Mbps
Average cost per node
—Moderately expensive
Media and connector size
—Medium to large
Maximum cable length
—100 m (short)
When comparing UTP and STP, keep the following points in mind:
The speed of both types of cable is usually satisfactory for local-area distances.
These are the least-expensive media for data communication. UTP is less expensive than STP. Because most buildings are already wired with UTP, many transmission standards are adapted to use it, to avoid costly rewiring with an alternative cable type.

Coaxial Cable

consists of a hollow outer cylindrical conductor that surrounds a single inner wire
made of two conducting elements. One of these elements, located in the center of the cable, is a copper conductor. Surrounding the copper conductor is a layer of flexible insulation. Over this insulating material is a woven copper braid or metallic foil that acts both as the second wire in the circuit and as a shield for the inner conductor. This second layer, or shield, can help reduce the amount of outside interference. Covering this shield is the cable jacket.

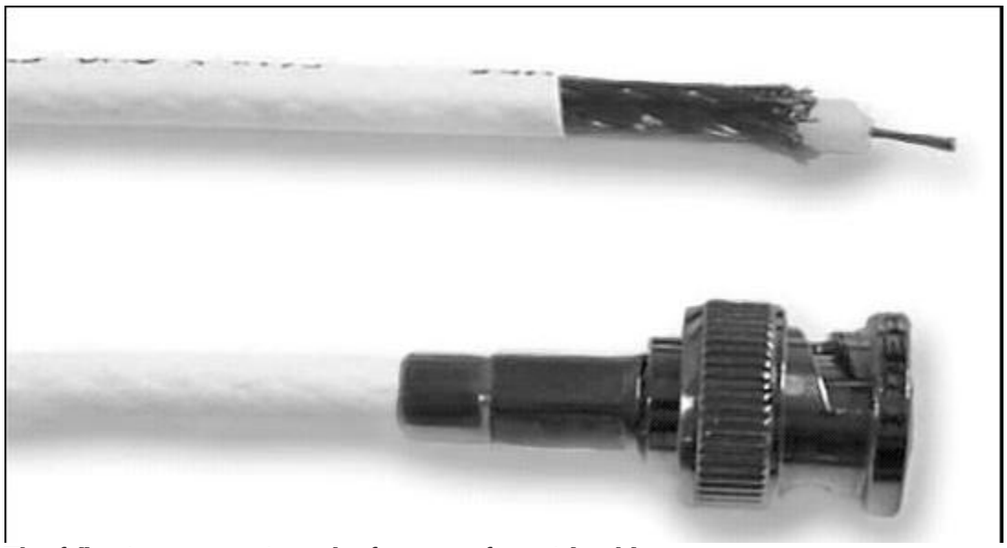


Coaxial cable supports 10 to 100 Mbps and is relatively inexpensive, although it is more costly than UTP on a per-unit length. However, coaxial cable can be cheaper for a physical bus topology because less cable will be needed. Coaxial cable can be cabled over longer distances than twisted-pair cable. For example, Ethernet can run approximately 100 meters (328 feet) using twisted-pair cabling. Using coaxial cable increases this distance to 500m (1640.4 feet). For LANs, coaxial cable offers several advantages. It can be run with fewer boosts from repeaters for longer distances between network nodes than either STP or UTP cable. Repeaters regenerate the signals in a network so that they can cover greater distances. Coaxial cable is less
expensive than fiber-optic cable, and the technology is well known; it has been used for many years for all types of data communication.

When working with cable, you need to consider its size. As the thickness, or diameter, of the cable increases, so does the difficulty in working with it. Many times cable must be pulled through existing conduits and troughs that are limited in size. Coaxial cable comes in a variety of sizes. The largest diameter (1 centimeter [cm]) was specified for use as Ethernet backbone cable because historically it had greater transmission length and noise-rejection characteristics. This type of coaxial cable is frequently referred to as *Thicknet*.

As its nickname suggests, Thicknet cable can be too rigid to install easily in some situations because of its thickness. The general rule is that the more difficult the network medium is to install, the more expensive it is to install. Coaxial cable is more expensive to install than twisted-pair cable. Thicknet cable is almost never used except for special-purpose installations. A connection device known as a *vampire tap* was used to connect network devices to Thicknet.

The vampire tap then was connected to the computers via a more flexible cable called the attachment unit interface (AUI). Although this 15-pin cable was still thick and tricky to terminate, it was much easier to work with than Thicknet. In the past, coaxial cable with an outside diameter of only 0.35 cm (sometimes referred to as *Thinnet*) was used in Ethernet networks. Thinnet was especially useful for cable installations that required the cable to make many twists and turns. Because it was easier to install, it was also cheaper to install. Thus, it was sometimes referred to as *Cheapernet* . However, because the outer copper or metallic braid in coaxial cable comprises half the electrical circuit, special care had to be taken to ensure that it was properly grounded. Grounding was done by ensuring that a solid electrical connection existed at both ends of the cable. Frequently, however, installers failed to properly ground the cable. As a result, poor shield connection was one of the biggest sources of connection problems in the installation of coaxial cable. Connection problems resulted in electrical noise, which interfered with signal transmittal on the networking medium. For this reason, despite its small diameter, Thinnet no longer is commonly used in Ethernet networks. The most common connectors used with Thinnet are BNC, short for British Naval Connector or Bayonet Neill Concelman, connectors (see Figure 8-5). The basic BNC connector is a male type mounted at each end of a cable. This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector. BNC T-connectors are female devices for connecting two cables to a network interface card (NIC). A BNC barrel connector facilitates connecting two cables together.



The following summarizes the features of coaxial cables:

Speed and throughput

—10 to 100 Mbps

Average cost per node

—Inexpensive

Media and connector size

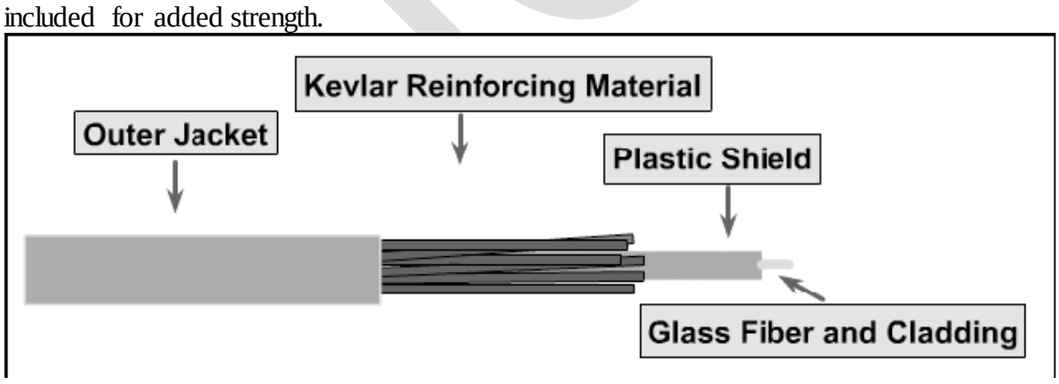
—Medium

Maximum cable length

—500 m (medium)

Fiber-Optic Cable

used for networking consists of two fibers encased in separate sheaths. If you were viewing it in a cross-section, you would see that each optical fiber is surrounded by layers of protective buffer material, usually a plastic shield, then a plastic such as Kevlar, and finally an outer jacket. The outer jacket provides protection for the entire cable, while the plastic conforms to appropriate fire and building codes. The Kevlar furnishes additional cushioning and protect on for the fragile, hair-thin glass fibers (see Figure 8-6). Wherever buried fiber-optic cables are required by codes, a stainless-steel wire sometimes is included for added strength.



The light-guiding parts of an optical fiber are called the *core* and the *cladding* . The core is usually very pure glass with a high index of refraction. When a cladding layer of glass or plastic with a low index of refraction surrounds the core glass, light can be trapped in the fiber core. This process is called *total internal reflection* . It allows the optical fiber to act like a light pipe guiding light for tremendous distances, even around bends. Fiber-optic cable is the most expensive of the four media discussed in this chapter, but it supports line speeds of more than 1 Gbps.

Two types of fiber-optic cable exist:

Single-mode

—Single-mode fiber cable allows only one mode (or wavelength) of light to propagate through the fiber. It is capable of higher bandwidth and greater distances than multimode, and it is often used for campus backbones. This type of fiber uses lasers as the light-generating method. Single-mode cable is much more expensive than multimode cable. Its maximum cable length is more than 10 km (32808.4 feet).

Multimode

—Multimode fiber cable allows multiple modes of light to propagate through the fiber. It is often used for workgroup applications and intrabuilding applications such

as risers. It uses light-emitting diodes (LEDs) as a light-generating device. The maximum cable length is 2 km (6561.7 feet).
The following summarizes the features of fiber-optic cables:
• **Speed and throughput**—More than 1 Gbps
• **Average cost per node**—Expensive
• **Media and connector size**—Small
• **Maximum cable length**—More than 10 km for single mode; up to 2 km for multimode

Wireless Transmission

Our age has given rise to information junkies: people who need to be on-line all the time. For these mobile users, twisted pair, coax, and fiber optics are of no use. They need to get their hits of data for their laptop, notebook, shirt pocket, palmtop, or wristwatch computers without being tethered to the terrestrial communication infrastructure. For these users, wireless communication is the answer. In the following sections, we will look at wireless communication in general, as it has many other important applications besides providing connectivity to users who want to surf the Web from the beach.

Some people believe that the future holds only two kinds of communication: fiber and wireless. All fixed (i.e., nonmobile) computers, telephones, faxes, and so on will use fiber, and all mobile ones will use wireless.

Wireless has advantages for even fixed devices in some circumstances. For example, if running a fiber to a building is difficult due to the terrain (mountains, jungles, swamps, etc.), wireless may be better. It is noteworthy that modern wireless digital communication began in the Hawaiian Islands, where large chunks of Pacific Ocean separated the users and the telephone system was inadequate.

Radio Transmission

Radio waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors. Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.

Sometimes omnidirectional radio is good, but sometimes it is bad. In the 1970s, General Motors decided to equip all its new Cadillacs with computer-controlled antilock brakes. When the driver stepped on the brake pedal, the computer pulsed the brakes on and off instead of locking them on hard. One fine day an Ohio Highway Patrolman began using his new mobile radio to call headquarters, and suddenly the Cadillac next to him began behaving like a bucking bronco. When the officer pulled the car over, the driver claimed that he had done nothing and that the car had gone crazy.

Eventually, a pattern began to emerge: Cadillacs would sometimes go berserk, but only on major highways in Ohio and then only when the Highway Patrol was watching. For a long, long time General Motors could not understand why Cadillacs worked fine in all the other states and also on minor roads in Ohio. Only after much searching did they discover that the Cadillac's wiring made a fine antenna for the frequency used by the Ohio Highway Patrol's new radio system.

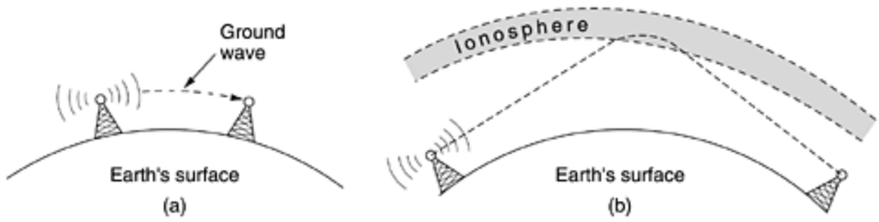
The properties of radio waves are frequency dependent. At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source, roughly as $1/r^2$ in air. At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles. They are also absorbed by rain. At all frequencies, radio waves are subject to interference from motors and other electrical equipment.

Due to radio's ability to travel long distances, interference between users is a problem. For this reason, all governments tightly license the use of radio transmitters, with one exception, discussed below.

In the VLF, LF, and MF bands, radio waves follow the ground, as illustrated in Fig. These waves can be detected for perhaps 1000 km at the lower frequencies, less at the

higher ones. AM radio broadcasting uses the MF band, which is why the ground waves from Boston AM radio stations cannot be heard easily in New York. Radio waves in these bands pass through buildings easily, which is why portable radios work indoors. The main problem with using these bands for data communication is their low bandwidth

Figure 2-12. (a) In the VLF, LF, and MF bands, radio waves follow the curvature of the earth. (b) In the HF band, they bounce off the ionosphere.



In the HF and VHF bands, the ground waves tend to be absorbed by the earth. However, the waves that reach the ionosphere, a layer of charged particles circling the earth at a height of 100 to 500 km, are refracted by it and sent back to earth, as shown in Fig. . Under certain atmospheric conditions, the signals can bounce several times. Amateur radio operators (hams) use these bands to talk long distance. The military also communicate in the HF and VHF bands.

Microwave Transmission

Above 100 MHz, the waves travel in nearly straight lines and can therefore be narrowly focused. Concentrating all the energy into a small beam by means of a parabolic antenna (like the familiar satellite TV dish) gives a much higher signal-to-noise ratio, but the transmitting and receiving antennas must be accurately aligned with each other. In addition, this directionality allows multiple transmitters lined up in a row to communicate with multiple receivers in a row without interference, provided some minimum spacing rules are observed. Before fiber optics, for decades these microwaves formed the heart of the long-distance telephone transmission system. In fact, MCI, one of AT&T's first competitors after it was deregulated, built its entire system with microwave communications going from tower to tower tens of kilometers apart. Even the company's name reflected this (MCI stood for Microwave Communications, Inc.). MCI has since gone over to fiber and merged with WorldCom.

Since the microwaves travel in a straight line, if the towers are too far apart, the earth will get in the way (think about a San Francisco to Amsterdam link). Consequently, repeaters are needed periodically. The higher the towers are, the farther apart they can be. The distance between repeaters goes up very roughly with the square root of the tower height. For 100-meter-high towers, repeaters can be spaced 80 km apart.

Unlike radio waves at lower frequencies, microwaves do not pass through buildings well. In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space. Some waves may be refracted off low-lying atmospheric layers and may take slightly longer to arrive than the direct waves. The delayed waves may arrive out of phase with the direct wave and thus cancel the signal. This effect is called multipath fading and is often a serious problem. It is weather and frequency dependent. Some operators keep 10 percent of their channels idle as spares to switch on when multipath fading wipes out some frequency band temporarily.

The demand for more and more spectrum drives operators to yet higher frequencies. Bands up to 10 GHz are now in routine use, but at about 4 GHz a new problem sets in: absorption by water. These waves are only a few centimeters long and are absorbed by rain. This effect would be fine if one were planning to build a huge outdoor microwave oven for roasting passing birds, but for communication, it is a severe problem. As with multipath fading, the only solution is to shut off links that are being rained on and route around them.

In summary, microwave communication is so widely used for long-distance telephone communication, mobile phones, television distribution, and other uses that a severe shortage of spectrum has developed. It has several significant advantages over fiber. The main one is that no right of way is needed, and by buying a small plot of ground every 50 km and putting a microwave tower on it, one can bypass the telephone system and communicate directly. This is how MCI managed to get started as a new long-distance telephone company so quickly. (Sprint went a completely different route: it was formed by the Southern Pacific Railroad, which already owned a large amount of right of way and just buried fiber next to the tracks.)

Microwave is also relatively inexpensive. Putting up two simple towers (may be just big poles with four guy wires) and putting antennas on each one may be cheaper than burying 50 km of fiber through a congested urban area or up over a mountain, and it may also be cheaper than leasing the telephone company's fiber, especially if the telephone company has not yet even fully paid for the copper it ripped out when it put in the fiber.

The Politics of the Electromagnetic Spectrum

To prevent total chaos, there are national and international agreements about who gets to use which frequencies. Since everyone wants a higher data rate, everyone wants more spectrum. National governments allocate spectrum for AM and FM radio, television, and mobile phones, as well as for telephone companies, police, maritime, navigation, military, government, and many other competing users. Worldwide, an agency of ITU-R (WARC) tries to coordinate this allocation so devices that work in multiple countries can be manufactured. However, countries are not bound by ITU-R's recommendations, and the FCC (Federal Communication Commission), which does the allocation for the United States, has occasionally rejected ITU-R's recommendations (usually because they required some politically-powerful group giving up some piece of the spectrum).

Even when a piece of spectrum has been allocated to some use, such as mobile phones, there is the additional issue of which carrier is allowed to use which frequencies. Three algorithms were widely used in the past. The oldest algorithm, often called the beauty contest, requires each carrier to explain why its proposal serves the public interest best. Government officials then decide which of the nice stories they enjoy most. Having some government official award property worth billions of dollars to his favorite company often leads to bribery, corruption, nepotism, and worse. Furthermore, even a scrupulously honest government official who thought that a foreign company could do a better job than any of the national companies would have a lot of explaining to do.

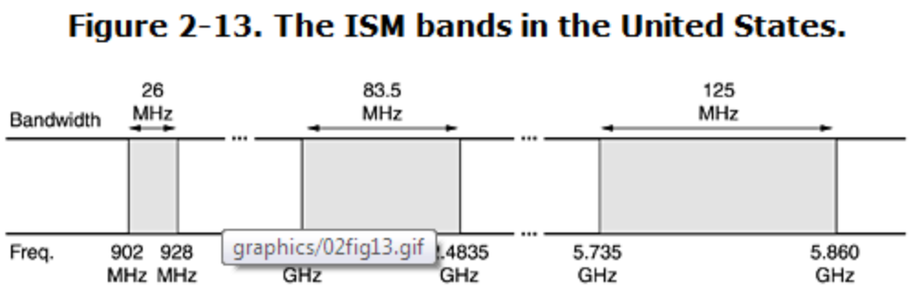
This observation led to algorithm 2, holding a lottery among the interested companies. The problem with that idea is that companies with no interest in using the spectrum can enter the lottery. If, say, a fast food restaurant or shoe store chain wins, it can resell the spectrum to a carrier at a huge profit and with no risk.

Bestowing huge windfalls on alert, but otherwise random, companies has been severely criticized by many, which led to algorithm 3: auctioning off the bandwidth to the highest bidder. When England auctioned off the frequencies needed for third-generation mobile systems in 2000, they expected to get about $4 billion. They actually received about $40 billion because the carriers got into a feeding frenzy, scared to death of missing the mobile boat. This event switched on nearby governments' greedy bits and inspired them to hold their own auctions. It worked, but it also left some of the carriers with so much debt that they are close to bankruptcy. Even in the best cases, it will take many years to recoup the licensing fee.

A completely different approach to allocating frequencies is to not allocate them at all. Just let everyone transmit at will but regulate the power used so that stations have such a short range they do not interfere with each other. Accordingly, most governments have set aside some frequency bands, called the ISM (Industrial, Scientific, Medical) bands for unlicensed usage. Garage door openers, cordless phones, radio-controlled toys, wireless mice, and numerous other wireless household devices use the ISM bands. To minimize interference between these uncoordinated devices, the FCC mandates that all devices in the ISM bands use spread spectrum techniques. Similar rules apply in other countries

The location of the ISM bands varies somewhat from country to country. In the United States, for example, devices whose power is under 1 watt can use the bands shown in Fig. without requiring a FCC license. The 900-MHz band works best, but it is crowded and not available worldwide. The 2.4-GHz band is available in most countries, but it is subject to interference from microwave ovens and radar installations. Bluetooth and some of the 802.11 wireless LANs operate in this band. The 5.7-GHz band is new and relatively undeveloped, so equipment for it is expensive, but since 802.11a uses it, it will quickly become more popular.

Figure 2-13. The ISM bands in the United States.



Infrared and Millimeter Waves

Unguided infrared and millimeter waves are widely used for short-range communication. The remote controls used on televisions, VCRs, and stereos all use infrared communication. They are relatively directional, cheap, and easy to build but have a major drawback: they do not pass through solid objects (try standing between your remote control and your television and see if it still works). In general, as we go from long-wave radio toward visible light, the waves behave more and more like light and less and less like radio.

On the other hand, the fact that infrared waves do not pass through solid walls well is also a plus. It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings: you cannot control your neighbor's television with your remote control. Furthermore, security of infrared systems against eavesdropping is better than that of radio systems precisely for this reason. Therefore, no government license is needed to operate an infrared system, in contrast to radio systems, which must be licensed outside the ISM bands. Infrared communication has a limited use on the desktop, for example, connecting notebook computers and printers, but it is not a major player in the communication game.

Lightwave Transmission

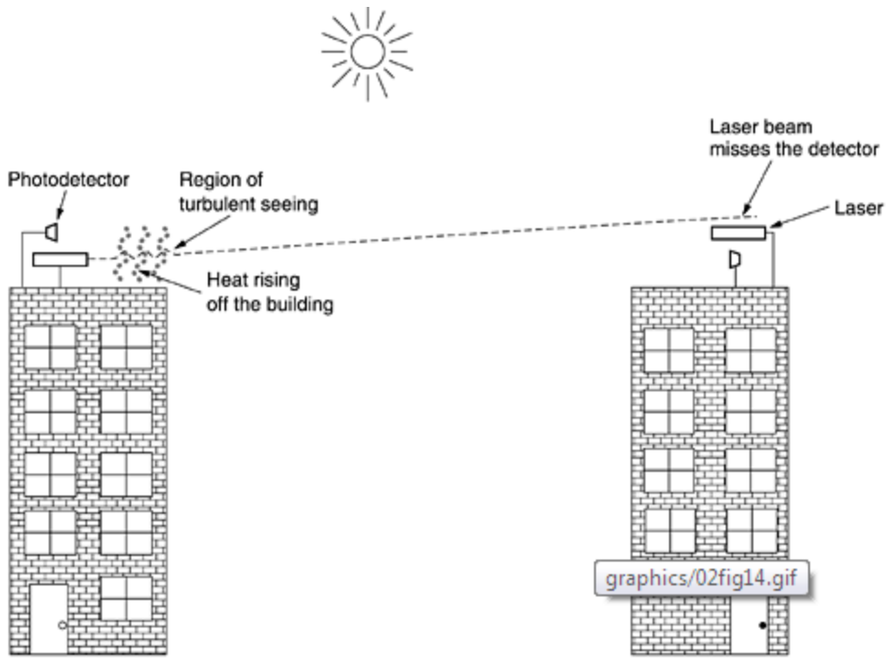
Unguided optical signaling has been in use for centuries. Paul Revere used binary optical signaling from the Old North Church just prior to his famous ride. A more modern application is to connect the LANs in two buildings via lasers mounted on their rooftops. Coherent optical signaling using lasers is inherently unidirectional, so each building needs its own laser and its own photodetector. This scheme offers very high bandwidth and very low cost. It is also relatively easy to install and, unlike microwave, does not require an FCC license.

The laser's strength, a very narrow beam, is also its weakness here. Aiming a laser beam 1-mm wide at a target the size of a pin head 500 meters away requires the marksmanship of a latter-day Annie Oakley. Usually, lenses are put into the system to defocus the beam slightly.

A disadvantage is that laser beams cannot penetrate rain or thick fog, but they normally work well on sunny days. However, the author once attended a conference at a modern hotel in Europe at which the conference organizers thoughtfully provided a room full of terminals for the attendees to read their e-mail during boring presentations. Since the local PTT was unwilling to install a large number of telephone lines for just 3 days, the

organizers put a laser on the roof and aimed it at their university's computer science building a few kilometers away. They tested it the night before the conference and it worked perfectly. At 9 a.m. the next morning, on a bright sunny day, the link failed completely and stayed down all day. That evening, the organizers tested it again very carefully, and once again it worked absolutely perfectly. The pattern repeated itself for two more days consistently.

After the conference, the organizers discovered the problem. Heat from the sun during the daytime caused convection currents to rise up from the roof of the building, as shown in Fig. . This turbulent air diverted the beam and made it dance around the detector. Atmospheric "seeing" like this makes the stars twinkle (which is why astronomers put their telescopes on the tops of mountains-to get above as much of the atmosphere as possible). It is also responsible for shimmering roads on a hot day and the wavy images seen when one looks out above a hot radiator.



Communication Satellites

In the 1950s and early 1960s, people tried to set up communication systems by bouncing signals off metallized weather balloons. Unfortunately, the received signals were too weak to be of any practical use. Then the U.S. Navy noticed a kind of permanent weather balloon in the sky-the moon-and built an operational system for ship-to-shore communication by bouncing signals off it.

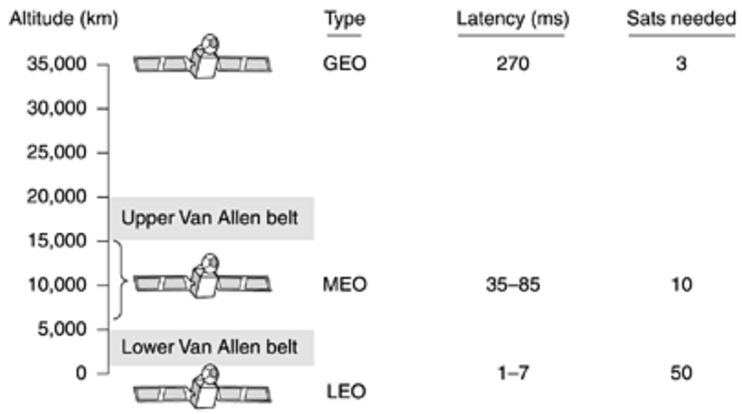
Further progress in the celestial communication field had to wait until the first communication satellite was launched. The key difference between an artificial satellite and a real one is that the artificial one can amplify the signals before sending them back, turning a strange curiosity into a powerful communication system.

Communication satellites have some interesting properties that make them attractive for many applications. In its simplest form, a communication satellite can be thought of as a big microwave repeater in the sky. It contains several transponders, each of which listens to some portion of the spectrum, amplifies the incoming signal, and then rebroadcasts it at another frequency to avoid interference with the incoming signal. The downward beams can be broad, covering a substantial fraction of the earth's surface, or narrow, covering an area only hundreds of kilometers in diameter. This mode of operation is known as a bent pipe.

According to Kepler's law, the orbital period of a satellite varies as the radius of the orbit to the 3/2 power. The higher the satellite, the longer the period. Near the surface of the earth, the period is about 90 minutes. Consequently, low-orbit satellites pass out of view fairly quickly, so many of them are needed to provide continuous coverage. At an altitude

of about 35,800 km, the period is 24 hours. At an altitude of 384,000 km, the period is about one month, as anyone who has observed the moon regularly can testify.

A satellite's period is important, but it is not the only issue in determining where to place it. Another issue is the presence of the Van Allen belts, layers of highly charged particles trapped by the earth's magnetic field. Any satellite flying within them would be destroyed fairly quickly by the highly-energetic charged particles trapped there by the earth's magnetic field. These factors lead to three regions in which satellites can be placed safely. These regions and some of their properties are illustrated in Fig. 2-15. Below we will briefly describe the satellites that inhabit each of these regions.



Types Of Connectors

1. RJ 45

RJ45 may refer to:

- A registered jack connector and wiring pattern used for connection of a high-speed modem to a telephone network using a keyed 8P8C modular connector
- An unkeyed 8P8C modular connector, often found on Ethernet cables

2. BNC

The **BNC connector (Bayonet Neill–Concelman)** is a common type of RF connector used for coaxial cable. It is used with radio, television, and other radio-frequency electronic equipment, test instruments, video signals, and was once a popular computer network connector. BNC connectors are made to match the characteristic impedance of cable at either 50 ohms or 75 ohms.

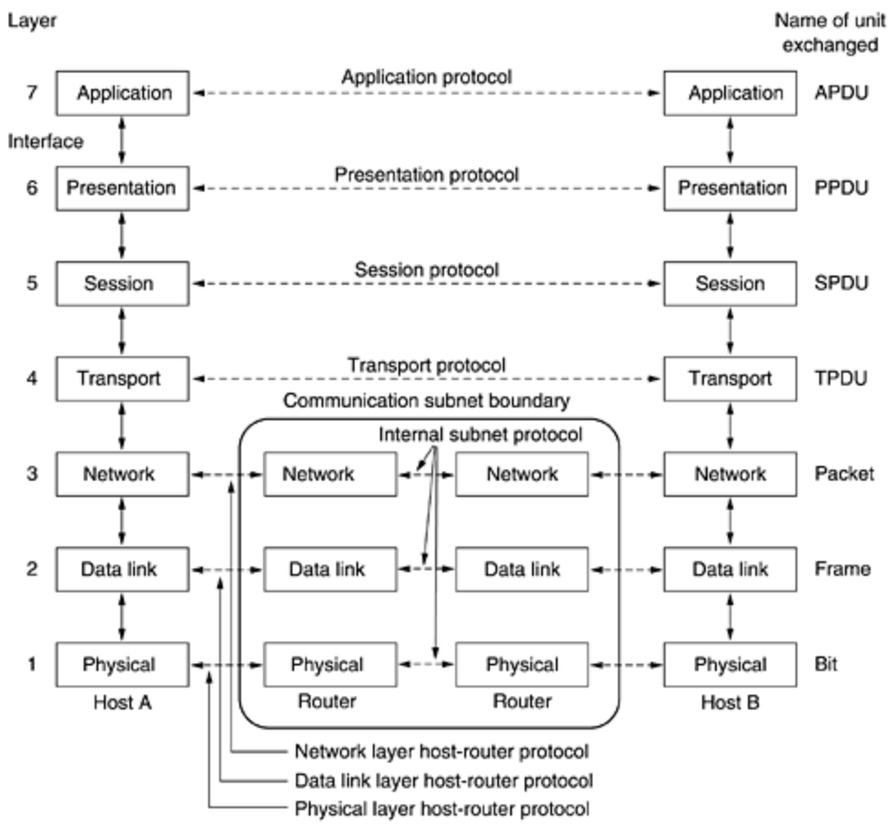
3. RJ 11

A **registered jack** (**RJ**) is a standardized physical network interface — both jack construction and wiring pattern — for connecting telecommunications or data equipment to a service provided by a local exchange carrier or long distance carrier. The standard designs for these connectors and their wiring are named **RJ11**, **RJ14**, **RJ21**, **RJ48**, etc. Many of these interface standards are commonly used in North America, though some interfaces are used world-wide.

What is OSI Model?

The OSI model (minus the physical medium) is shown in Fig. 1-20. This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995 (Day, 1995). The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems-that is, systems that are open for communication with other systems. We will just call it the OSI model for short.

Figure 1-20. The OSI reference model.



The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

Below we will discuss each layer of the model in turn, starting at the bottom layer. Note that the OSI model itself is not a network architecture because it does not specify the exact services and protocols to be used in each layer. It just tells what each layer should do. However, ISO has also produced standards for all the layers, although these are not part of the reference model itself. Each one has been published as a separate international standard.

The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions here are how many volts should be used to represent a 1 and how many for a 0, how many nanoseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established and how it is torn down when both sides are finished, and how many pins the network connector has and what each pin is used for. The design issues here largely deal with mechanical, electrical, and timing interfaces, and the physical transmission medium, which lies below the physical layer.

The Data Link Layer

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often needed to let the transmitter know how much buffer space the receiver has at the moment. Frequently, this flow regulation and the error handling are integrated.

Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel. A special sublayer of the data link layer, the medium access control sublayer, deals with this problem.

The Network Layer

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. The control of such congestion also belongs to the network layer. More generally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.

When a packet has to travel from one network to another to get to its destination, many problems can arise. The addressing used by the second network may be different from the first one. The second one may not accept the packet at all because it is too large. The protocols may differ, and so on. It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.

In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The Transport Layer

The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology.

The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network. The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the

order in which they were sent. However, other possible kinds of transport service are the transporting of isolated messages, with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations. The type of service is determined when the connection is established. (As an aside, an error-free channel is impossible to achieve; what people really mean by this term is that the error rate is low enough to ignore in practice.)

The transport layer is a true end-to-end layer, all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages. In the lower layers, the protocols are between each machine and its immediate neighbors, and not between the ultimate source and destination machines, which may be separated by many routers. The difference between layers 1 through 3, which are chained, and layers 4 through 7, which are end-to-end, is illustrated in Fig. 1-20.

The Session Layer

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (checkpointing long transmissions to allow them to continue from where they were after a crash).

The Presentation Layer

Unlike lower layers, which are mostly concerned with moving bits around, the presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

The Application Layer

The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

PROTOCOLS IN NETWORKING

A **communications protocol** is a system of digital message formats and rules for exchanging those messages in or between computing systems and in telecommunications. A protocol may have a formal description.

Protocols may include signaling, authentication and error detection and correction capabilities.

A protocol definition defines the syntax, semantics, and synchronization of communication; the specified behavior is typically independent of how it is to be implemented. A protocol can therefore be implemented as hardware or software or both.

Few common protocols are.

1. ftp
2. http

3. nwlink
4. nntp
5. netbeui
6. tcp/ip

1. Ftp:

File Transfer Protocol (**FTP**) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server.

2. HTTP:

The **Hypertext Transfer Protocol** (**HTTP**) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web

3. NWLINK:

NWLink IPX/SPX/NetBIOS Compatible Transport is Microsoft's implementation of the Novell IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) protocol stack. The Windows XP implementation of the IPX/SPX protocol stack adds NetBIOS support. The main function of NWLink is to act as a transport protocol to route packets through internetworks. By itself, the NWLink protocol does not allow you to access the data across the network. If you want to access NetWare File and Print Services, you must install NWLink and Client Services for NetWare (software that works at the upper layers of the OSI model to allow access to File and Print services). One advantage of using NWLink is that is easy to install and configure.

4. NNTP:

The **Network News Transfer Protocol** (**NNTP**) is an Internet application protocol used for transporting Usenet news articles (*netnews*) between news servers and for reading and posting articles by end user client applications. Brian Kantor of the University of California, San Diego and Phil Lapsley of the University of California, Berkeley authored RFC 977, the specification for the Network News Transfer Protocol, in March 1986. Other contributors included Stan O. Barber from the Baylor College of Medicine and Erik Fair of Apple Computer.

5. NETBEUI:

NetBIOS is an acronym for **Network Basic Input/Output System**. It provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.

6. TCP/IP:

TCP/IP is the communication protocol for communication between computers on the Internet.

TCP/IP stands for **T**ransmission **C**ontrol **P**rotocol / **I**nternet**P**rotocol.

TCP/IP defines how electronic devices (like computers) should be connected to the Internet, and how data should be transmitted between them

TCP

TCP is for communication between applications.

If one application wants to communicate with another via TCP, it sends a communication request. This request must be sent to an exact address. After a "handshake" between the two applications, TCP will set up a "full-duplex" communication between the two applications.

The "full-duplex" communication will occupy the communication line between the two computers until it is closed by one of the two applications.

UDP is very similar to TCP, but simpler and less reliable.

IP:

The Transmission Control Protocol/Internet Protocol is a network communication protocol. It can be used as a communications protocol on private networks and it is the default protocol in use on the internet. When you set up any system to have direct access to the Internet, whether it is via dial-up or one of the high speed technologies in use today, your system will need to utilize the TCP/IP protocol whether it is a Windows based system or not.

Also, if the given system needs to communicate to other TCP/IP systems on the local LAN or WAN it will need to utilize the TCP/IP protocol as well.

TCP/IP version 4 (IPv4) addresses are made of up four 8-bit fields (octets) and are 32-bits in size total. Microsoft TCP/IP version 4 supports the standard classes of address, which defines which bits are used for the network ID and which bits are used for the host ID. There are five TCP/IP version 4 (IPv4) addresses, although for the most part, only the A, B, and C classes are used. The system of IP address classes described here form the basis for IP address assignment. Classless Inter-Domain Routing (CIDR) addressing is now being used more often and I will cover that later in the article. Classless Inter-Domain Routing is making the IP address classes in their current for "less defined", for lack of a better term. Still, the classes form the base of any addressing scheme.

TCP/IP version 4 address are made of both a network ID and a host ID. The network ID address identifies the physical network where the hosts exist. The host ID address identifies the individual TCP/IP host on a network. The host ID must be unique on the internal network, that is, no two nodes on a given network can have the same network ID AND host ID.

TCP/IP version 6 (IPv6) addresses are a set of specifications from the Internet Engineering Task Force (IETF) and has been designed to overcome the current shortage of addresses under TCP/IP version 4. TCP/IP version 6 also has some other built in improvements that goes beyond the scope of the discussion here. The single most important thing you will need to know for the 70-270 exam (a little more depth may be needed for the upcoming Exam 70-275: Installing, Configuring and Administering Microsoft .NET Server and Exam 70-276: Implementing and Administering

a Microsoft .NET Server Network Infrastructure) is that IPv6 addresses are 128 bits in length as opposed to 32 bits under IPv4.

Subnet Masks - Implementing subnewtorks (commonly referred to as subnets in the field) helps to control network traffic. Every node on the same physical Ethernet network sees all the packets of data sent out on the network. Often this has the result of multiple collisions causing network performance to be slow. Routers or gateways are used to separate networks into subnets. Subnet masks on each of the nodes allow the nodes on the same subnetwork to continue to communicate with one another and to the routers or gateways they use to send their messages.

Network Address : 158.21.0.0
Subnet Mask : 255.255.0.0

CLASSES OF IP ADRESSES:

TCP/IP Class A Address Overview

The "A" class addressing scheme has an official start address of 0.0.0.0 and an official last address of 127.255.255.255.

Not all of these address can be used and you will OFTEN see conflicting information on this.1.0.0.1 to 126.255.255.254 is the range of IP addresses that are included in the "A" class addressing scheme that are the useable range for node assignment126.255.255.255 is a broadcast address and in most case cannot be assigned. (There are exceptions to the rule.)

The local host will use 0.0.0.0 when it cannot reach a DHCP server when it is set to use one and cannot assign itself an address using APIPA.1.0.0.1 to 126.255.255.254 is the useable range.

There are 126 Class A networks total, each allowed to have up to 16,777,214 hosts The 127.x.x.x range is used for internal host loopback There are three IP network addresses reserved for private networks. 10.0.0.0 -10.255.255.255 with the subnet mask 255.0.0.0 is the range for Class A IP addresses.

They can be used by anyone setting up internal IP networks, such as a lab or home LAN behind a NAT or proxy server or a router. It is always safe to use these because routers on the Internet will never forward packets coming from these addresses.

These addresses are defined in RFC 1918.
While 10.0.0.0 - 10.255.255.255 addresses with the subnet mask 255.0.0.0 are available to only internal IP networks, they are still considered part of the Class "A" range.

TCP/IP Class B Address Overview

The "B" class addressing scheme has an official start address of 128.0.0.0 and an official last address of 191.255.255.255.Not all of these address can be used and you will OFTEN see conflicting information on this.128.0.0.1 to 191.255.255.254 is the range of IP addresses that are included in the "B" class addressing scheme that are the useable range for node assignment. The local host will use 0.0.0.0 when it cannot reach a DHCP server when it is set to use one and cannot assign itself an address using APIPA.
There are three IP network addresses reserved for private networks. 172.16.0.0 - 172.31.255.255 with the subnet mask 255.240.0.0 is the range for Class B IP addresses.
They can be used by anyone setting up internal IP networks, such as a lab or home LAN behind a NAT or proxy server or a router. It is always safe to use these because routers on the Internet will never forward packets coming from these addresses.
These addresses are defined in RFC 1918. While 172.16.0.0 - 172.31.255.255 addresses with the subnet mask 255.240.0.0 are available to only internal IP networks, they are still considered part of the Class "B" range.

TCP/IP Class C Address Overview

The "C" class addressing scheme has an official start address of 192.0.0.0 and an official last address of 223.255.255.255.
Not all of these address can be used and you will OFTEN see conflicting information on this. 192.0.0.1 to 223.255.255.254 is the range of IP addresses that are included in the "C" class addressing scheme that are the useable range for node assignment.
The local host will use 0.0.0.0 when it cannot reach a DHCP server when it is set to use one and cannot assign itself an address using APIPA. There are three IP network addresses reserved for private networks. 192.168.0.0 -192.168.255.255 with the subnet mask 255.255.0.0 is the range for Class C IP addresses.They can be used by anyone setting up internal IP networks, such as a lab or homeLAN behind a NAT or proxy server or a router. It is always safe to use these because routers on the Internet will never forward packets coming from these addresses.
These addresses are defined in RFC 1918. While 192.168.0.0 - 192.168.255.255 addresses with the subnet mask 255.255.0.0 are available to only internal IP networks, they are still considered part of the Class "C"range.

TCP/IP Class D Address Overview

The IP version 4 addresses of 224.0.0.0 through 239.255.255.255 are set aside through IANA (Internet Assigned Numbers Authority) as a special class of addresses for Multicast uses. At the present, ISPs are unable to allocate Class D address space to their customers. These addresses must be allocated through IANA.
Class D addresses are only required if you wish to be a multicast source. You can still receive multicast data without the need for a separate Class D address.

TCP/IP Class E Address Overview

The IP version 4 addresses of 240.0.0.0 to 254.255.255.255 are set aside through IANA (Internet Assigned Numbers Authority) as a special class of addresses for experimental and future use.
The IP address of 255.255.255.255 broadcasts to all hosts on the local network and therefore, is not to be considered as part of the E class of IP addresses.
"The fact that the grass is greener on the other side of the fence is directly proportional to how much manure is being used on the property"

Practical Portion

PRACTICAL #1: INSTALLING AND CONFIGURING MODEM

Modem overview

Telephone lines that are used in a conventional phone system are designed to transmit human speech with analog signals. Analog signals vary continuously, like waves, along their length. Computers store and process data in digital format and communicate both internally and with each other in binary digits.

When two computers communicate with each other over a conventional phone line, a modem translates the binary information from the computer at the sending end to an analog signal that can pass over the phone line. At the receiving end, another modem translates the analog signal back to binary information that can be used by the computer. The conversion from binary to analog information is called *modulation* and the conversion back from analog to binary is called *demodulation*. The word *modem*, short for modulator/demodulator, is the name for the device that performs these conversions.

Both standard modems and fax machines perform this conversion. When you communicate over analog telephone lines, you use standard modems. There are also ISDN and cable modems that provide digital communication. They enable computers to transmit digital information directly without the conversion over special lines. The most recent developments with the fastest transmissions are broadband technologies such as cable or DSL (Digital Subscriber Line) that transmit over cable or phone lines as waves similar to radio or television.

Installing a modem

To install the modem hardware on your computer, refer to the manufacturer's documentation. Generally, the following instructions apply:

- If you have an internal modem with jumpers, set the jumpers for Plug and Play for the Windows Server 2003 family or, if that option is unavailable, for Windows 95, Windows 98, Windows NT, Windows 2000, or Windows Millennium Edition.
- Install an internal modem in an empty slot. Attach an external serial modem to an unused COM port.
- If you have an external modem, ensure that it is attached to the computer, plugged into the power source, and turned on before you turn on the computer and start Windows.
- Ensure that your modem is properly connected to the phone line and to your computer.

Most modems manufactured now are compatible with Plug and Play and installed automatically after they are connected to the computer. However, older modems and external serial modems may not be detected. If your modem is not installed automatically, then use **Phone and Modem Options** in **Control Panel** to install it manually. To install a modem, see Install a modem. To choose the modem type manually, see Install an unsupported modem.

Setting hardware connections

A modem has to be connected to the telephone system and to a power source.

Telephone connections
Both internal and external modems use a modular phone cord, called an RJ-11 coupler. Usually, a new modem includes the coupler. If you have an older, four-pronged jack, you may also need an adapter to connect to your phone line.

If your office has digital, PBX or multiline phones, you cannot connect a modem directly to the phone system. You need to either install a standard line or install a device that connects your modem to one of these systems. See your computer or telephone supplier for specialized solutions.

Power connections
Internal modems are powered directly by the computer. External modems usually come with a power adapter, but are sometimes powered by the computer. Most portable modems for portable computers use batteries, although they often come with an adapter too. Some are powered directly from the computer. Modems use different sizes and styles of adapters, so if you lose the adapter, you need to get a new one from the modem or computer manufacturer. Refer to the manufacturer's documentation for additional information about the power requirements of your computer.

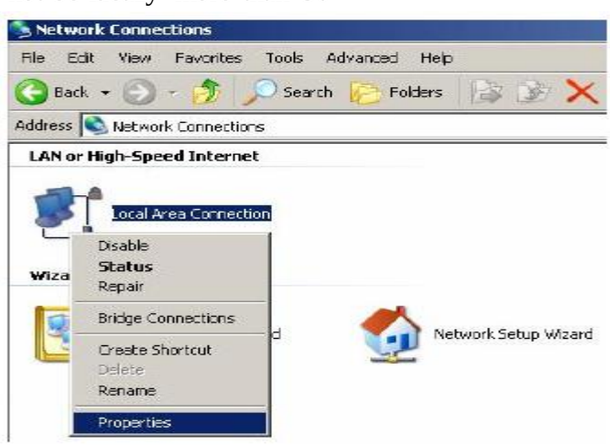
Cabling Connections
External serial modems connect to the computer with a serial cable, also called an RS-232 cable. If a cable is not provided with your modem, make sure you get one that fits both your computer's serial port and the modem's port.

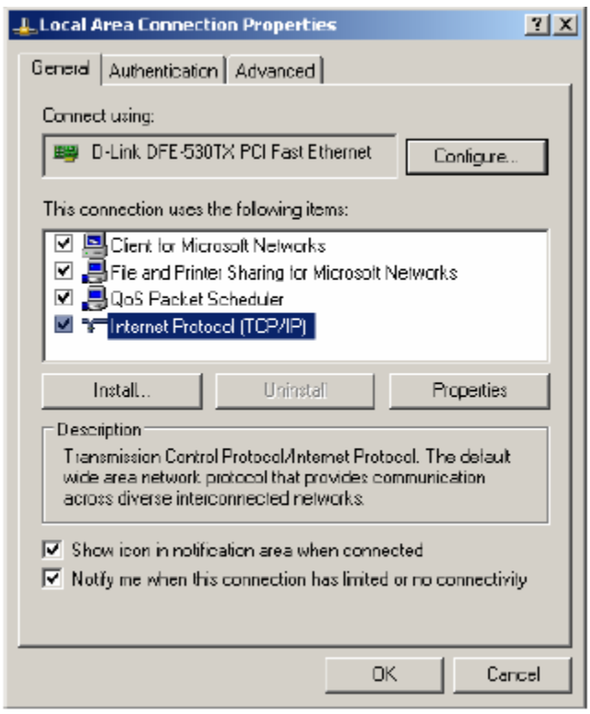
Practical #2: DSL CONFIGURATION

Step 1: Connecting to the Splitter, Power Connection & LAN cable.
1 Line hole connects to PTCL wire or Wall phone Jack (RJ-11 Jack).
2 Modem hole connects to the DSL jack of the ADSL CPE (Customer Premises Equipment).
3 Phone hole connects to a telephone set.
4 Connect the Power Adapter to the AC power plug and attach the connector of adapter to the CPE and switch it on.
5 Attach one end of LAN wire (RJ-45) to the LAN interface of CPE and the other end to the LAN wire to the LAN interface of computer's LAN card.
6 Link Indicator lights will lit up and show the connectivity. ADSL light will start blinking and soon will be static as a sign of connectivity with our system, if the line is properly jumpered in PTCL premises with the DSLAM (Digital Subscriber Line Access Multiplexer).Joint less and direct cable line from the nearest PTCL pole or cabinet must be connecting to your splitter and then all the phone extensions must be taken from the phone hole of splitter. The Drop wire distance from PTCL pole or Cabinet must not be ideally more than 50 meters.(Twisted pair wire can be longer)

Step 2: ADSL Configuration in CPE and Computer

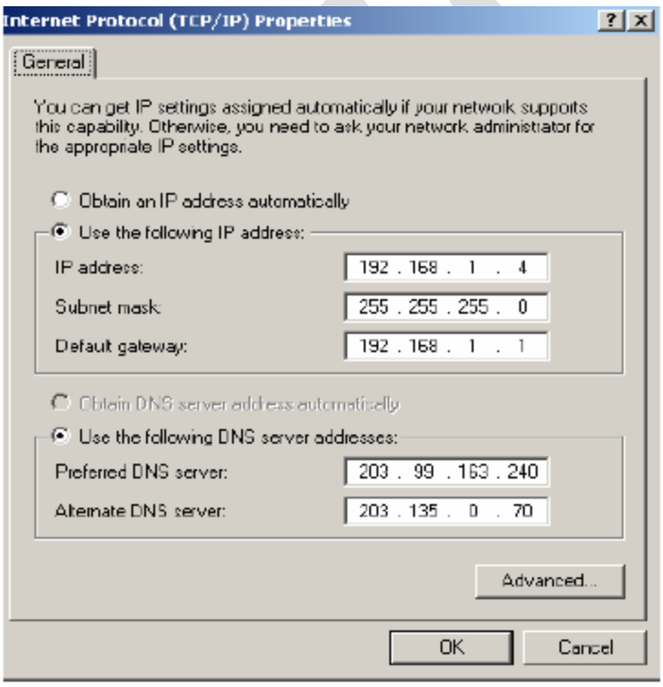
1. Go to Start Menu < Control Panel < Network and Internet Connections < Network Connections. Check that the Local Area Connection is enabled. Right click local Area network and click properties. Following window will be shown.



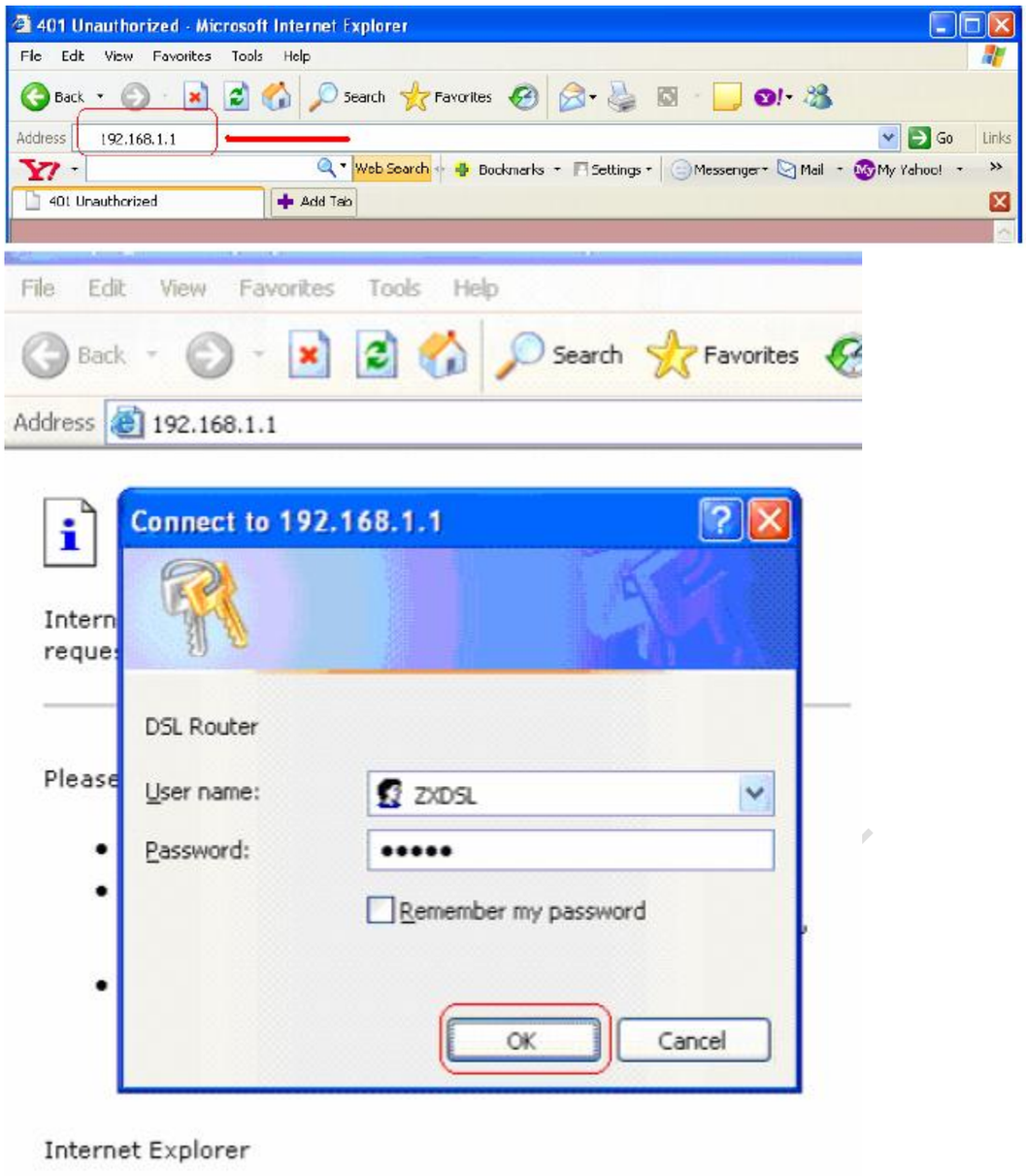


Double click "internet protocol (TCP/IP)", Check **"Use the following IP address"** and make the following settings:
IP Address: 192.168.1.3
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1
Then, check **"Use the following DNS server addresses"** and make the following settings:
Preferred DNS Server: 203.99.163.240

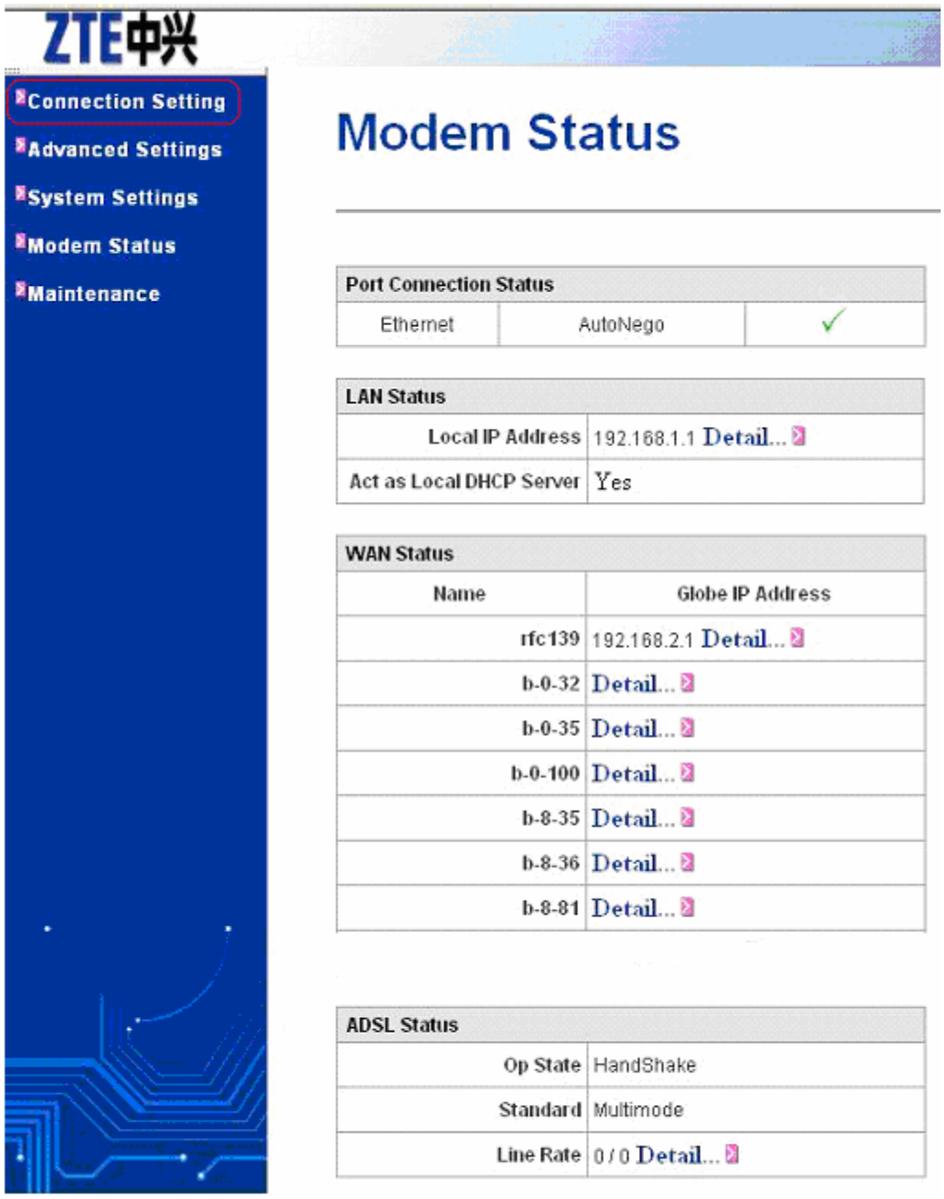
Alternate DNS Server: 203.135.0.170



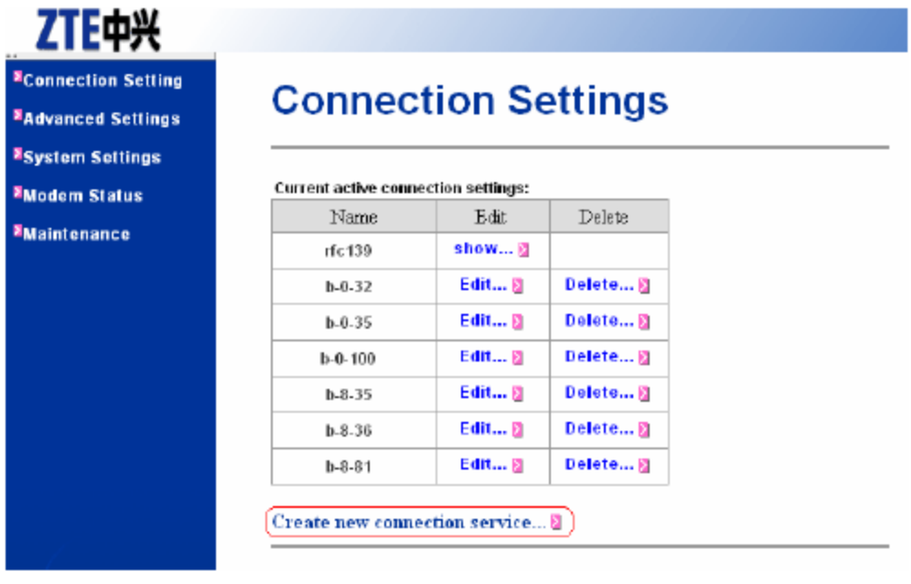
3. Now open Internet Explorer and write "**192.168.1.1"** in address bar and press enter. There must not be any proxy setting in the internet Explorer.
A small pop up window will open as shown in the figure below and ask **"User Name"** and **"Password"** for opening the CPE's interface.
Enter **User Name: ZXDSL** and **Password: ZXDSL** and press OK.
Note: "Both username & password must be written in capital letters."



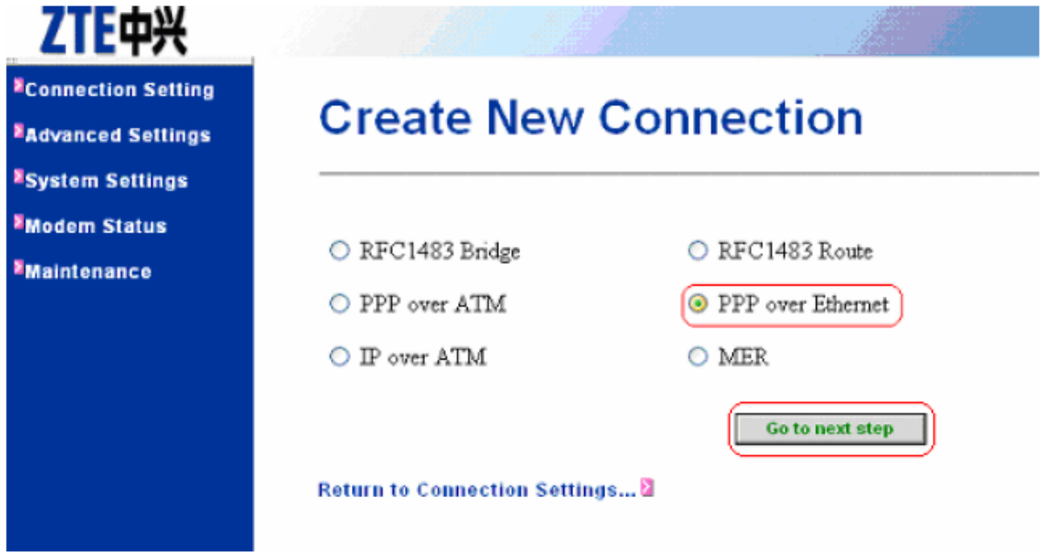
4. CPE configuration will be opened. This will show Modem Status. Click the **Connection Setting.**



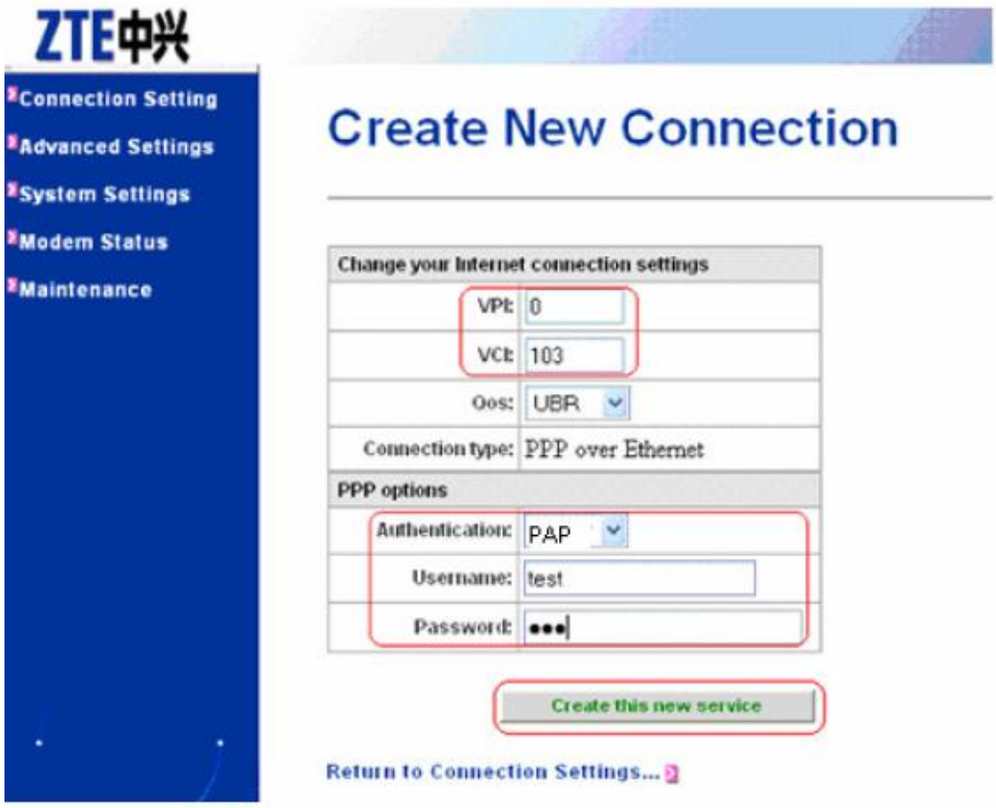
5. Connection Settings show current active connection as shown in the figure. Click **create new connection service**



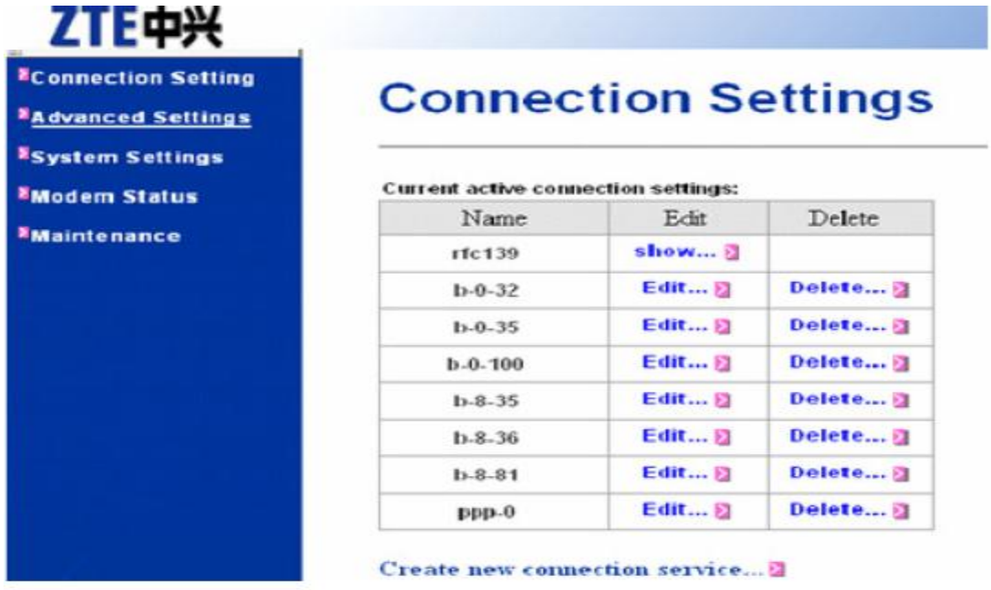
6. In create new connection window. Select "**PPP over Ethernet"**



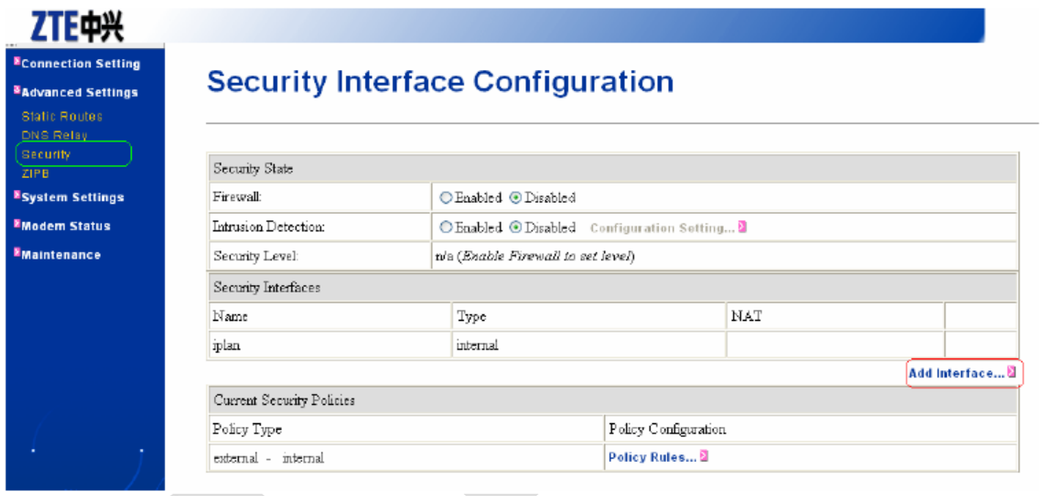
7. Enter **VPI=0** and **VCI=103** for Copper number & **VPI=8** and **VCI=81** for ONU Fiber Optics number. Select Authentication protocol as "**PAP"** and enter username and Password. Click "**Create this new service"**.



8. Now Connection settings window will be opened and shows current active connections

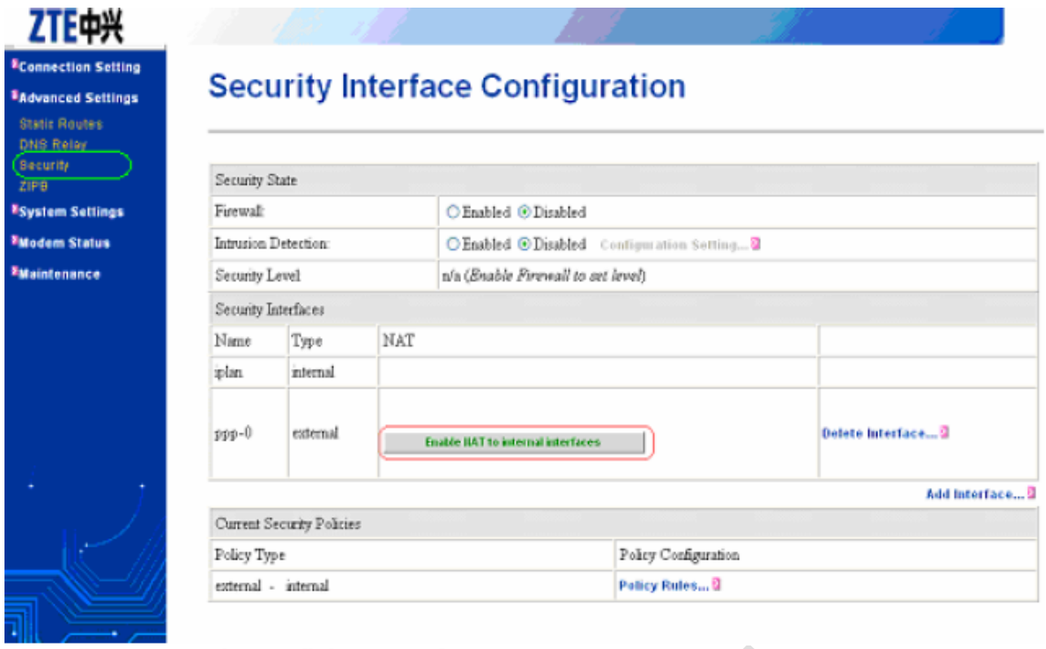


9. Click **Advance settings** and then on **Security** .Security Interface Configuration is shown. Click **Add Interface.**

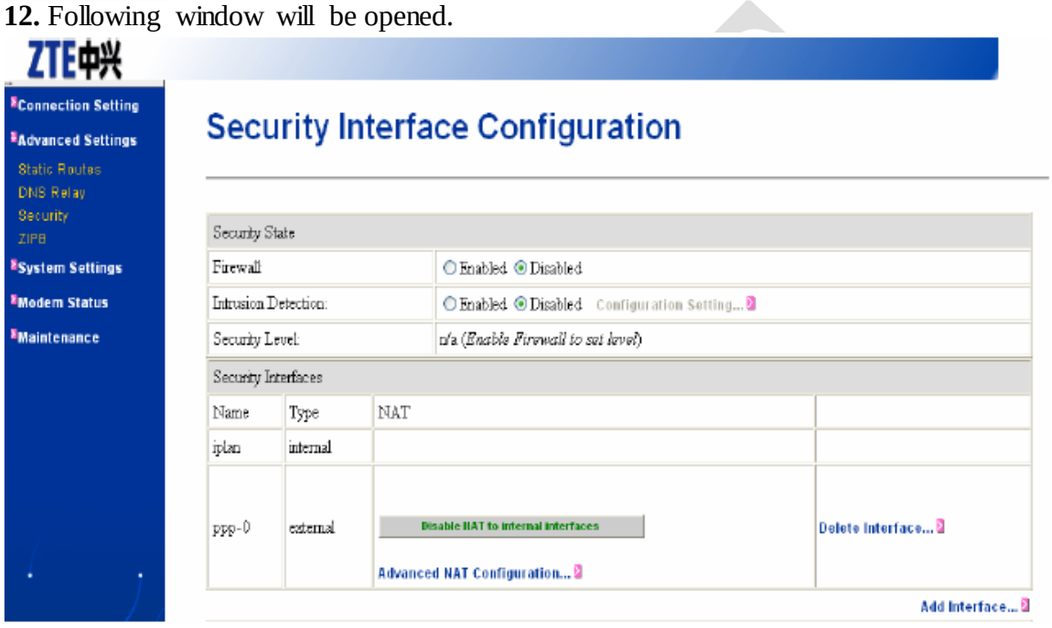


10. Following figure will be shown. Click **Apply**.

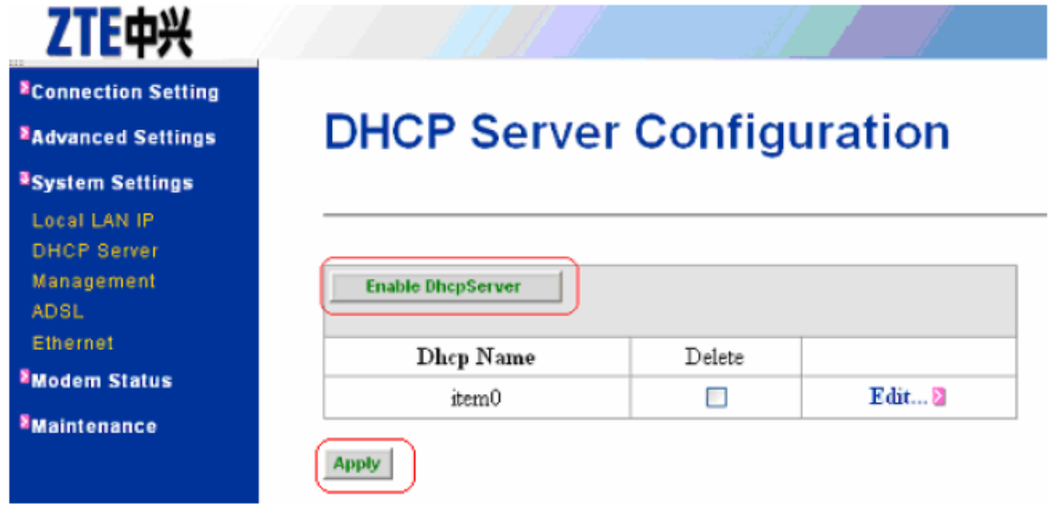
11. Security Interface Configuration will be opened. Click **Enable NAT to interface**.



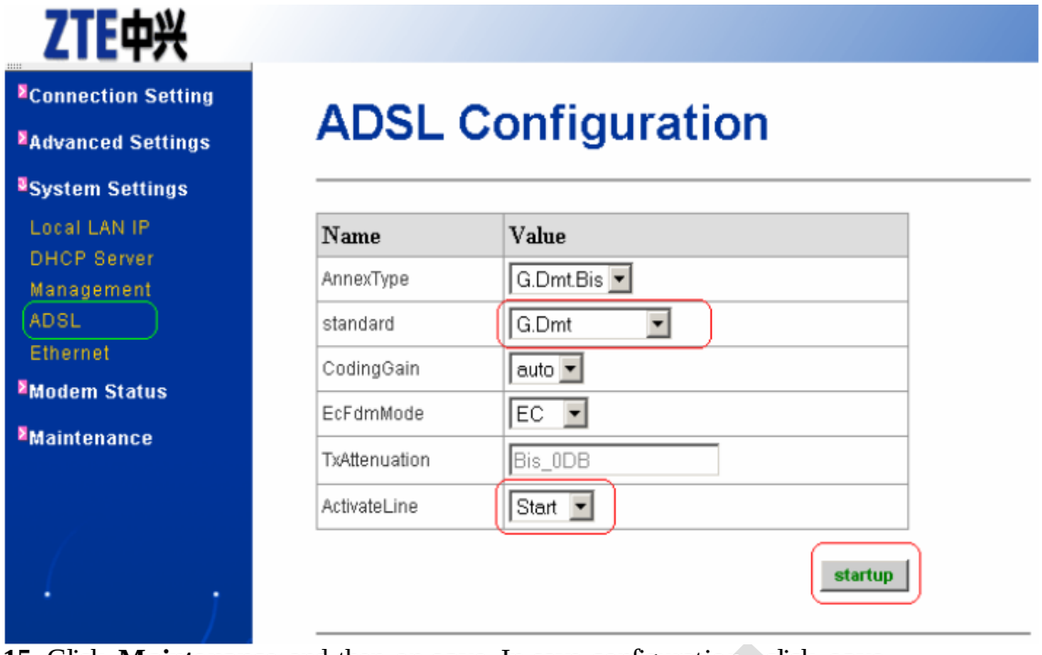
12. Following window will be opened.



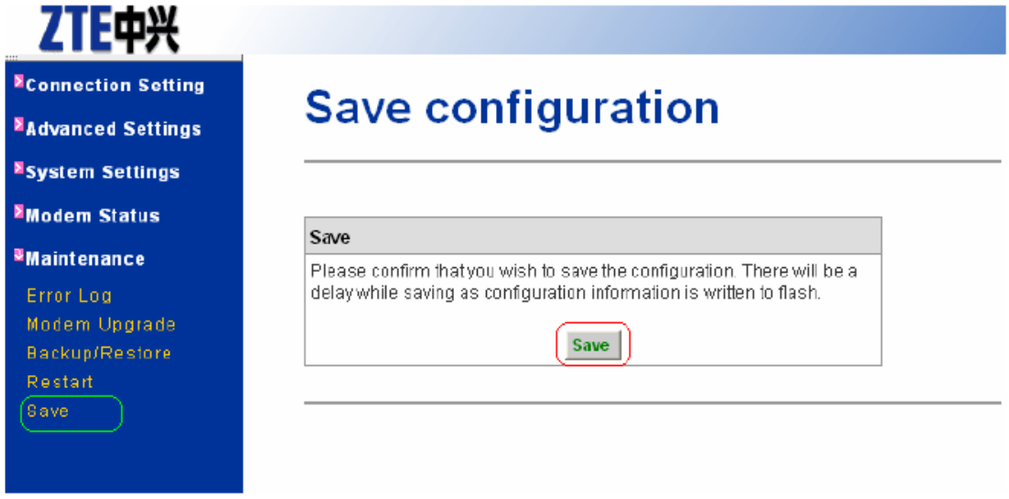
13. Click **System Settings** and then on **DHCP Server**. In DHCP Server Configuration, Click on **Enable DHCPServer** and **Apply**



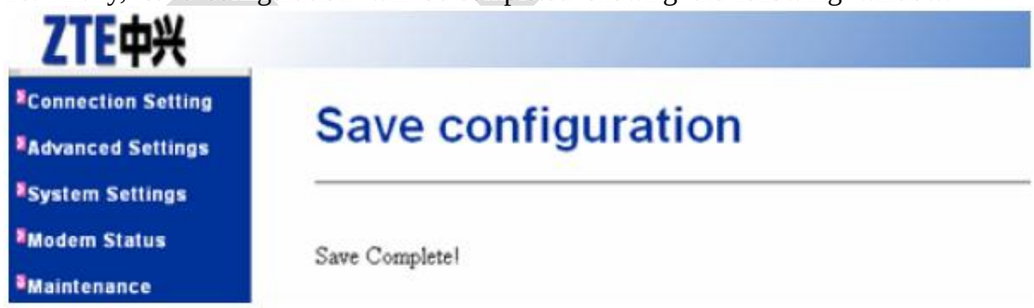
14. Click on **ADSL.** ADSL Configuration Window will be opened. Select **Standard: G.DmtBisPlus** and **ActiveLine: Start**. Click **Startup.**



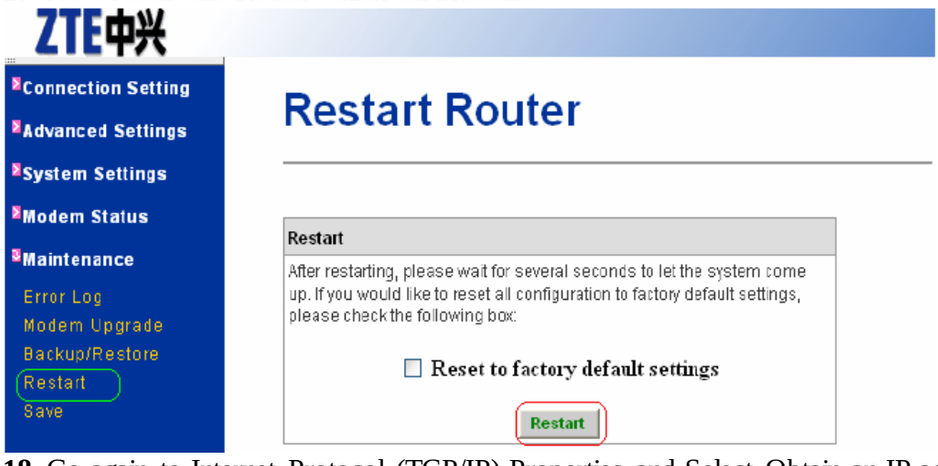
15. Click **Maintenance** and then on **save.** In save configuration, click **save**



16. Finally, save configuration will be completed showing the following window.

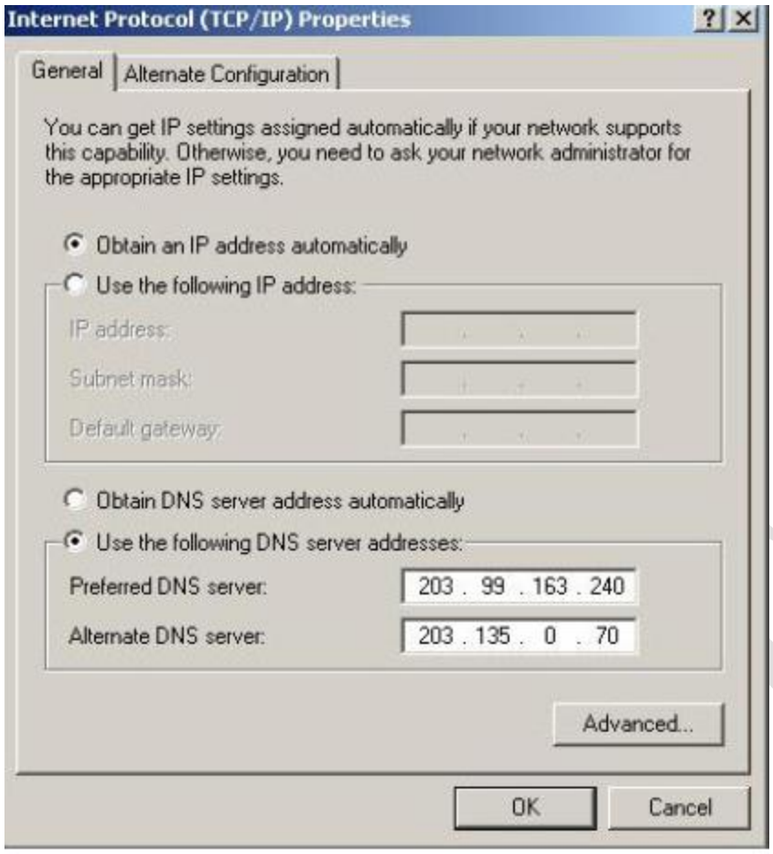


17. Now restart the Router. Click on **Restart.**



18. Go again to Internet Protocol (TCP/IP) Properties and Select Obtain an IP address automatically and leave the DNS server addresses unchanged as shown in the picture

below and press Ok.
Now, open the Internet Explorer and start browsing the sites for successful configuration and
DSL connection establishment.

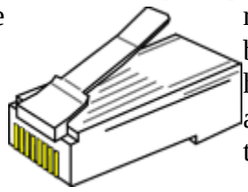


Practical#3:Creating Straight Through,Cross cable,RollOver Cables

NETWORK CABLE AND CONNECTORS

There are several classifications of cable used for twisted-pair networks. I'll skip right over them and state that I use and recommend Category 5 (or CAT 5) cable for all new installations. Likewise, there are several fire code classifications for the outer insulation of CAT 5 cable. I use CMR cable, or "riser cable," for most of the wiring I do. You should also be aware of CMP or plenum cable (a plenum is used to distribute air in a building). You may be required by local, state or national codes to use the more expensive plenum-jacketed cable if it runs through suspended ceilings, ducts, or other areas, if they are used to circulate air or act as an air passage from one room to another. If in doubt, use plenum. CMR cable is generally acceptable for all applications not requiring plenum cable.

CAT 5 wire is available in reel-in-box packaging. This is very handy for pulling the wire without putting twists in it. Without this kind of package or a cable reel stand, pulling wire is a two-person job. Before the advent of the reel-in-box, we used to put a reel of wire on a broom handle to pull it. One person would hold the broom handle and the other would pull and measure the cable. You will produce a tangled mess, if you pull the wire off the end of the reel.



Stranded wire patch cables are often specified for cable segments running from a wall jack to a PC and for patch panels. They are more flexible than solid core wire. However,

the rational for using it is that the constant flexing of patch cables may wear-out solid core cable--break it. I don't think this is a real concern in the average small network. For example, I have one solid core cable going to my work bench. It has probably flexed and average person's lifetime of flexes from the many many times I have connected customer computers to my network. Also, stranded cable is susceptible to degradation from moisture infiltration, may use an alternate color code, and should not be used for cables longer than 3 Meters (about 10 feet).

Most of the wiring I do simply connects computers directly to other computers or hubs. Solid core cable is quite suitable for this purpose and for many home and small business networks. I find it also quite acceptable for use as patch cables. You might consider a stranded wire patch cable if you have a notebook computer you are constantly moving around.

CAT 5 cable has four twisted pairs of wire for a total of eight individually insulated wires. Each pair is color coded with one wire having a solid color (blue, orange, green, or brown) twisted around a second wire with a white background and a stripe of the same color. The solid colors may have a white stripe in some cables. Cable colors are commonly described using the background color followed by the color of the stripe; e.g., white-orange is a cable with a white background and an orange stripe.

CONNECTORS. The straight through and cross-over patch cables discussed in this article are terminated with CAT 5 RJ-45 modular plugs. RJ-45 plugs are similar to those you'll see on the end of your telephone cable except they have eight versus four or six contacts on the end of the plug and they are about twice as big. Make sure they are rated for CAT 5 wiring. (RJ means "Registered Jack"). Also, there are RJ-45 plugs designed for both solid core wire and stranded wire. Others are designed specifically for one kind of wire or the other. Be sure you buy plugs appropriate for the wire you are going to use. I use plugs designed to accommodate both kinds of wire.

NETWORK CABLE TOOLS

Last updated: 2/11/2000

Modular Plug Crimp Tool. You will need a modular crimp tool. This one is very similar to the one I have been using for many years for all kinds of telephone cable work and it works just fine for Ethernet cables. You don't need a lot of bells and whistles, just a tool which will securely crimp RJ-45 connectors. This one is made by Eclipse Enterprises, Inc. Even though the crimper has cutters which can be used to cut the cable and individual wires, and possibly stripping the outer jacket, I find that the following tools are better for stripping and cutting the cable...

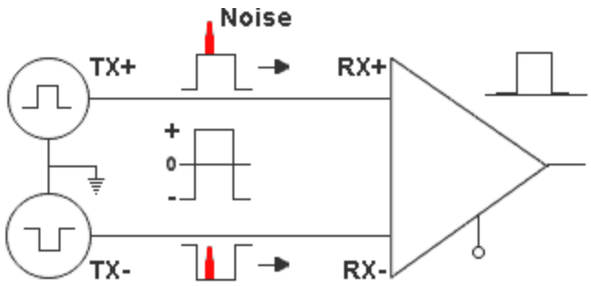
Universal UTP Stripping Tool (Eclipse). I recently bought one of these tools and it works slick, and it makes a much neater cut. I recommend that you purchase one if you will be making many cables.

Diagonal Cutters ("4 to 6"). It is easier to use diagonal cutters ("diags" or "dikes") to cut the cable off at the reel and to fine tune the cable ends during assembly. Also, if you don't have a stripper, you can strip the cable by using a small knife (X-acto, utility, etc.) to carefully slice the outer jacket longitudinally and use the diags to cut it off around the circumference.

A LITTLE THEORY

Now, bear with me, you need to understand some of this stuff...

The 10BASE-T and 100BASE-TX Ethernets consist of two transmission lines. Each transmission line is a pair of twisted wires. One pair receives data signals and the other pair transmits data signals. A balanced line driver or transmitter is at one end of one of these lines and a line receiver is at the other end. A (much) simplified schematic for one of these lines and its transmitter and receiver follow:



Pulses of energy travel down the transmission line at about the speed of light (186,000 miles/second). The principal components of one of these pulses of energy is the voltage potential between wires and current flowing near the surface of the wires. This energy can also be considered as residing in the magnetic field which surrounds the wires and the electric field between the wires. In other words, an electromagnetic wave which is guided by, and travels down the wires.

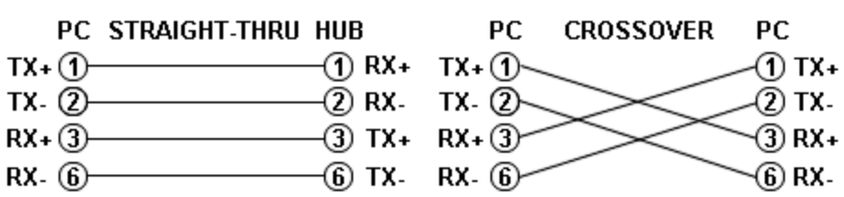
The main concern is the transient magnetic fields which surrounds the wires and the magnetic fields generated externally by the other transmission lines in the cable, other network cables, electric motors, fluorescent lights, telephone and electric lines, lightning, etc. This is known as noise. Magnetic fields induce their own pulses in a transmission line which may literally bury the Ethernet pulses, the conveyor of the information being sent down the line.

The twisted-pair Ethernet employs two principle means for combating noise. The first is the use of balanced transmitters and receivers. A signal pulse actually consists of two simultaneous pulses relative to ground: a negative pulse on one line and a positive pulse on the other. The receiver detects the total difference between these two pulses. Since a pulse of noise (shown in red in the diagram) usually produces pulses of the same polarity on both lines one pulse is essentially canceled by out the other at the receiver. Also, the magnetic field surrounding one wire from a signal pulse is a mirror of the one on the other wire. At a very short distance from the two wires the magnetic fields are opposite and have a tendency to cancel the effect of each other out. This reduces the line's impact on the other pair of wires and the rest of the world.

The second and the primary means of reducing cross-talk--the term cross-talk came from the ability to (over) hear conversations on other lines on your phone--between the pairs in the cable, is the double helix configuration produced by twisting the wires together. This configuration produces symmetrical (identical) noise signals in each wire. Ideally, their difference, as detected at the receiver, is zero. In actuality it is much reduced.

COLOR-CODE STANDARDS

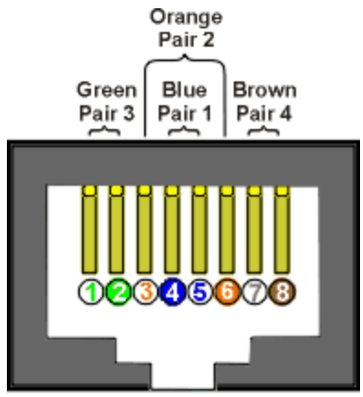
Again, please bear with me... Let's start with simple pin-out diagrams of the two types of UTP Ethernet cables and watch how committees can make a can of worms out of them. Here are the diagrams:



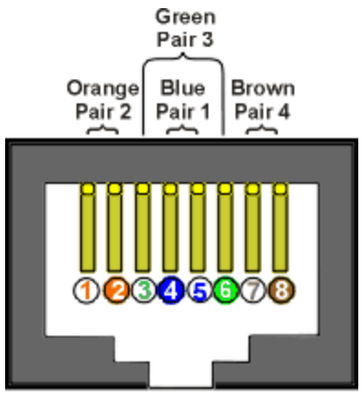
Note that the TX (transmitter) pins are connected to corresponding RX (receiver) pins, plus to plus and minus to minus. And that you must use a crossover cable to connect

units with identical interfaces. If you use a straight-through cable, one of the two units must, in effect, perform the cross-over function.

Two wire color-code standards apply: EIA/TIA 568A and EIA/TIA 568B. The codes are commonly depicted with RJ-45 jacks as follows (the view is from the front of the jacks):

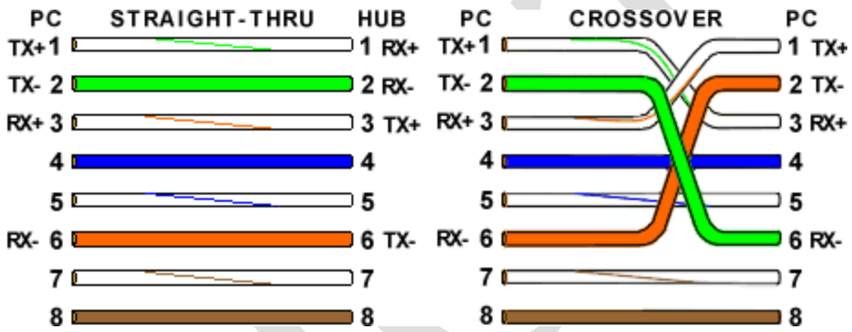


RJ-45 JACK
EIA/TIA 568A STANDARD



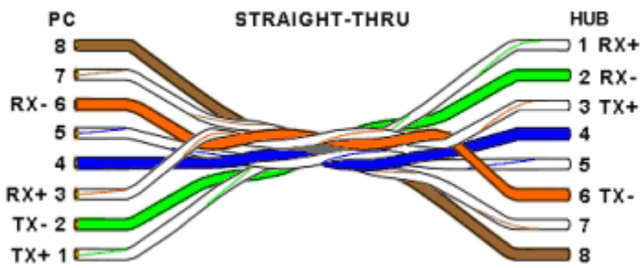
RJ-45 JACK
EIA/TIA 568B STANDARD

If we apply the 568A color code and show all eight wires, our pin-out looks like this:



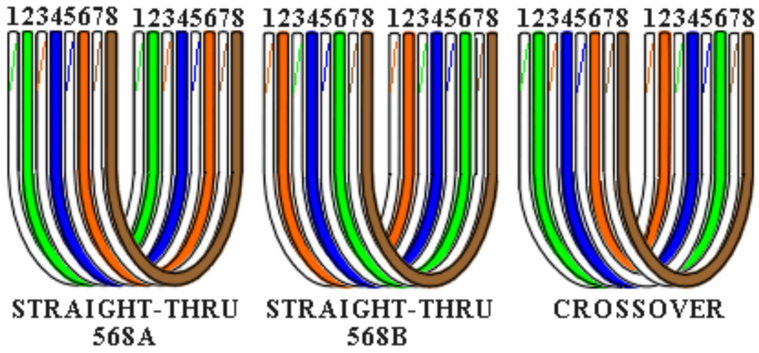
Note that pins 4, 5, 7, and 8 and the blue and brown pairs are not used in either standard. Quite contrary to what you may read elsewhere, these pins and wires are not used or required to implement 100BASE-TX duplexing--they are just plain wasted.

However, the actual cables are not physically that simple. In the diagrams, the orange pair of wires are not adjacent. The blue pair is upside-down. The right ends match RJ-45 jacks and the left ends do not. If, for example, we invert the left side of the 568A "straight"-thru cable to match a 568A jack--put one 180° twist in the entire cable from end-to-end--and twist together and rearrange the appropriate pairs, we get the following can-of-worms:



This further emphasizes, I hope, the importance of the word "twist" in making network cables which will work. You cannot use an flat-untwisted telephone cable for a network cable. Furthermore, you must use a pair of twisted wires to connect a set of transmitter pins to their corresponding receiver pins. You cannot use a wire from one pair and another wire from a different pair.

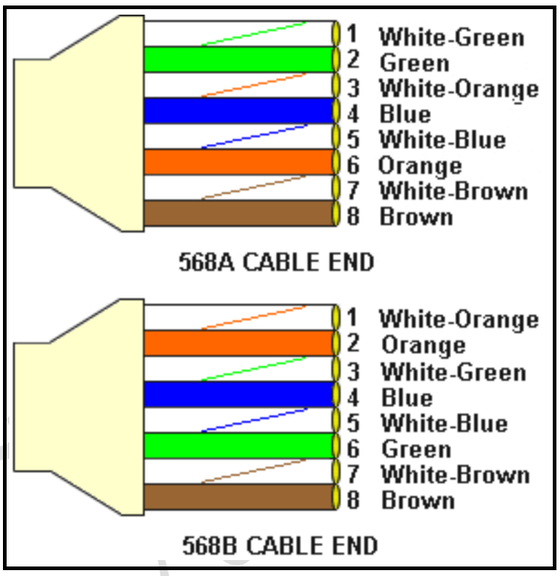
Keeping the above principles in mind, we can simplify the diagram for a 568A straight-thru cable by untwisting the wires, except the 180° twist in the entire cable, and bending the ends upward. Likewise, if we exchange the green and orange pairs in the 568A diagram we will get a simplified diagram for a 568B straight-thru cable. If we cross the green and orange pairs in the 568A diagram we will arrive at a simplified diagram for a crossover cable. All three are shown below.



LET'S MAKE IT SIMPLE

Last updated: 8/17/2000

There are only two unique cable ends in the preceding diagrams. They correspond to the 568A and 568B RJ-45 jacks and are shown to the right.



Again, the wires with colored backgrounds may have white stripes and may be denoted that way in diagrams found elsewhere. For example, the green wire may be labeled Green-White--I don't bother. The background color is always specified first.

Now, all you need to remember, to properly configure the cables, are the diagrams for the two cable ends and the following rules:

- **A straight-thru cable has identical ends.**
- **A crossover cable has different ends.**

It makes no functional difference which standard you use for a straight-thru cable. You can start a crossover cable with either standard as long as the other end is the other standard. It makes no functional difference which end is which. Despite what you may have read elsewhere, a 568A patch cable will work in a network with 568B wiring and 568B patch cable will work in a 568A network. The electrons couldn't care less.

My preference is to use the 568A standard for straight-thru cables and to start crossover cables with a 568A end. That way all I have to remember is the diagram for the 568A end, that a straight-thru cable has two of them, and that the green and orange pairs are swapped at the other end of a crossover cable.

LET'S MAKE SOME CABLES

Last updated: 5/20/02

1. Pull the cable off the reel to the desired length and cut. I have a box of cable at one end of my shop and a mark on the floor 10' away. For cable lengths which are a fraction of ten feet, I eye-ball the length as I pull the cable out of the box (also, my feet are about one foot long). For longer cables, I pull it out to the ten foot mark and go back to the box and pull the remaining fraction or another ten feet. If you are pulling cables through walls, a hole in the floor, etc., it easier to attach the RJ-45 plugs after the cable is pulled. The total length of wire segments between a PC and a hub or between two PC's cannot exceed 100 Meters (328 feet or about the length of a football field) for 100BASE-TX (and 10BASE-T).

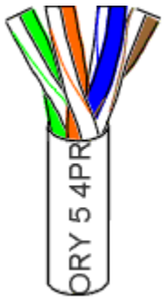
2. Strip one end of the cable with the stripper or a knife and diags. If you are using the stripper, place the cable in the groove on the blade (left) side of the stripper and align the end of the cable with the right side of the stripper. This

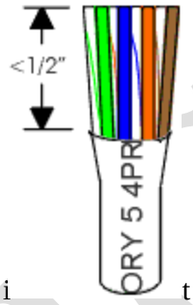
is about right to strip a little over 1/2" of the jacket off the cable. Turn the stripper about one turn or so. If you turn it much more, you will probably nick the wires. The idea is to score the outer jacket, but not go all the way through. Once scored, you should be able to twist the end of the jacket loose and pull it off with one hand while holding the rest of the cable with the other. If you are using a knife and diags, carefully slit the cable for about an inch or so and neatly trim around the circumference of the cable with the diags to remove the jacket.

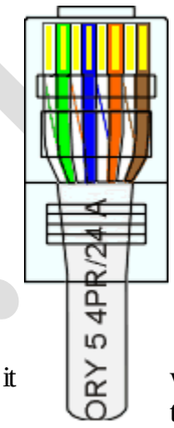
3. Inspect the wires for nicks. Cut off the end and start over if you see any. You may have to adjust the blade with the screw at the front stripper. Cable diameters and jacket thicknesses vary.

4. Spread and arrange the pairs roughly in the order of the desired cable end.

5. Untwist the pairs and arrange the wires in the order of the desired cable end. Flatten the end between your thumb and forefinger. Trim the ends of the wires so they are even with one another. **It is very important that the unstripped (untwisted) end be slightly less than 1/2"**





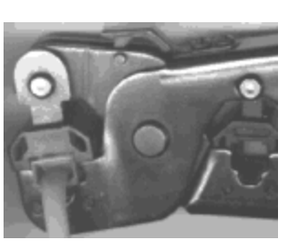


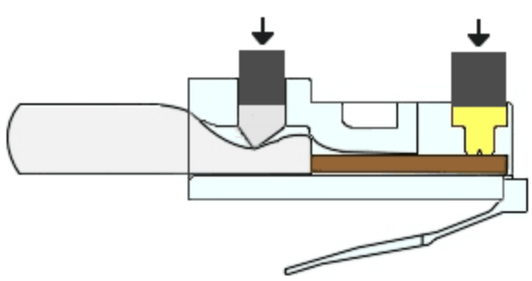
long. If it is longer than 1/2" it will be out-of-spec and susceptible to crosstalk. If it less than slightly less than 1/2" it will not be properly clinched when RJ-45 plug is crimped on.. Flatten again. There should be little or no space between the wires.

6. Hold the RJ-45 plug with the clip facing down or away from you. Push the wire firmly into the plug. **Now, inspect the darn thing... before crimping and wasting the plug!** Looking through the bottom of the plug, the wire on the far left side will have a white background. The wires should alternate light and dark from left to right. The furthest right wire is brown. The wires should all end evenly at the front of the plug. The jacket should end just about where you see it in the diagram--right on the line. Aren't you glad you didn't crimp the plug?

ALL ABOUT CRIMPING
Last updated: 2/11/2000

7. Hold the wire near the RJ-45 plug with the clip down and firmly push it into the left side of the front of the crimper (it will only go in one way). Hold the wire in place squeeze the crimper handles quite firmly. This is what will happen:





(Crimp it once.) The crimper pushes two plungers down on the RJ-45 plug. One forces what amounts to a cleverly designed plastic plug/wedge onto the cable jacket and very

firmly clinches it. The other seats the "pins," each with two teeth at its end, through the insulation and into the conductors of their respective wires.

8. Test the crimp... If done properly an average person will not be able to pull the plug off the cable with his or her bare hands. And that quite simply, besides lower cost, is the primary advantage of twisted-pair cables over the older thinwire, coaxial cables. In fact, I would say the RJ-45 and ease of its installation is the main reason coaxial cable is no longer widely used for small Ethernets. But, don't pull that hard on the plug. It could stretch the cable and change its characteristics. Look at the side of the plug and see if it looks like the diagram and give it a fairly firm tug to make sure it is crimped well.

9. Prepare the other end of the cable so it has the desired end and crimp.

10. If both ends of the cable are within reach, hold them next to each other and with RJ-45 clips facing away. Look through the bottom of the plugs. If the plugs are wired correctly, and they are identical, it is a straight-thru cable. If they are wired correctly and they are different, it is a crossover cable.

11. If you have an operational network, test the cable. Copy some large files.

12. If the cable doesn't work, inspect the ends again and make sure you have the right cable and that it is plugged into the correct units for the type of cable. Try power-cycling (cold booting) the involved computers.

13. If you have many straight-thru cables and a crossover cable in your system, you should consider labeling the crossover cable or using a different colored cable for the crossover cable so you don't mix them up. I do not recommend implementing the crossover function, as recommended elsewhere, with two RJ-45 jacks, appropriately wired back to back, and two straight-thru cables. This method costs noticeably more, introduces more than the necessary number of components and connections, increases the complexity and time of assembly, and decreases reliability.

CABLING RULES

Last updated: 2/23/2003

1. Try to avoid running cables parallel to power cables.

2. Do not bend cables to less than four times the diameter of the cable.

3. If you bundle a group of cables together with cable ties (zip ties), do not over-cinch them. It's okay to snug them together firmly; but don't tighten them so much that you deform the cables.

4. Keep cables away from devices which can introduce noise into them. Here's a short list: copy machines, electric heaters, speakers, printers, TV sets, fluorescent lights, copiers, welding machines, microwave ovens, telephones, fans, elevators, motors, electric ovens, dryers, washing machines, and shop equipment.

5. Avoid stretching UTP cables (tension when pulling cables should not exceed 25 LBS).

6. Do not run UTP cable outside of a building. It presents a very dangerous lightning hazard!

7. Do not use a stapler to secure UTP cables. Use telephone wire/RG-6 coaxial wire hangers which are available at most hardware stores.

Practical#4:Basic Commands for Troubleshooting
Ping, ipconfig / all, ipconfig / renew, ipconfig / release, trace route,

PING - Ping can be used to test your TCP/IP connection by sending a message to the remote node or gateway from a local system. (It can also be used to test the loopback locally only to see if it is working correctly.) If the remote node or gateway

receives the message, it responds with a reply message. The reply consists of the remote's IP address, the number of bytes in the message, how long it took to reply- given in milliseconds (ms), the length of time-to-live (TTL) in seconds and it will also show any pack loss in terms of percentages.

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] target_name

Switches:

- -t Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
- -a Resolve addresses to hostnames.
- -n count Number of echo requests to send.
- -l size Send buffer size.
- -f Set Don't Fragment flag in packet.
- -i TTL Time To Live.
- -v TOS Type Of Service.
- -r count Record route for count hops.
- -s count Timestamp for count hops.
- -j host-list Loose source route along host-list.
- -k host-list Strict source route along host-list.
- -w timeout Timeout in milliseconds to wait for each reply.

ARP - Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

- -a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
- -g Same as -a.
- inet_addr Specifies an internet address.
- -N if_addr Displays the ARP entries for the network interface specified by if_addr.
- -d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.
- -s Adds the host and associates the Internet address inet_addr with the Physical address
- eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
- eth_addr Specifies a physical address.
- if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.

IPCONFIG - Use the ipconfig command to get the local system's basic IP configuration information, including the IP address, subnet mask, and default gateway.

The IPCONFIG/all switch produces a detailed configuration report for all interfaces, including any configured remote access adapters.

USAGE: ipconfig [/? | /all | /renew [adapter] | /release [adapter] | /flushdns | /displaydns | /registerdns | /showclassid adapter | /setclassid adapter [classid]]

- /all Display full configuration information.
- /release Release the IP address for the specified adapter.
- /renew Renew the IP address for the specified adapter.
- /flushdns Purges the DNS Resolver cache.
- /registerdns Refreshes all DHCP leases and re-registers DNS names
- /displaydns Display the contents of the DNS Resolver Cache.
- /showclassid Displays all the dhcp class IDs allowed for adapter.
- /setclassid Modifies the dhcp class id.

The default is to display only the IP address, subnet mask and default gateway for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address leases for all adapters bound to TCP/IP will be released or renewed.

NBTSTAT - NetBT Statistics (Nbtstat.exe) is used for troubleshooting network NetBIOS names over TCP/IP (NetBT) resolution problems from the command line. It displays protocol statistics and current TCP/IP connections that are using NetBT.

When a network is functioning, NetBT resolves NetBIOS names to IP addresses. It uses several options for NetBIOS name resolution, including local cache lookup, WINS server query, broadcast, Lmhosts and Hosts file lookup, and DNS server query.

Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).

NBTSTAT [[-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]]

- -a (adapter status) Lists the remote machine's name table given its name
- -A (Adapter status) Lists the remote machine's name table given its IP address.
- -c (cache)Lists NBT's cache of remote [machine] names and their IP addresses
- -n (names)Lists local NetBIOS names.
- -r (resolved) Lists names resolved by broadcast and via WINS
- -R (Reload) Purges and reloads the remote cache name table
- -S (Sessions) Lists sessions table with the destination IP addresses
- -s (sessions) Lists sessions table converting destination IP addresses to computer NETBIOS names.
- -RR(ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

- RemoteName - Remote host machine name.
- IP address - Dotted decimal representation of the IP address.
- interval - Redisplays selected statistics, pausing interval seconds between each display. Press Ctrl+C to stop redisplaying statistics.

NETSTAT - Netstat (Netstat.exe) displays TCP/IP protocol statistics and active connections to and from your computer from the command line and also provides an option to display the number of bytes sent and received, as well as network packets dropped (if any).

NETSTAT [-a] [-e] [-n] [-o] [-s] [-p proto] [-r] [interval]

- -a Displays all connections and listening ports.
- -e Displays Ethernet statistics. This may be combined with the -s option.
- -n Displays addresses and port numbers in numerical form.
- -o Displays the owning process ID associated with each connection.
- -p proto Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP TCPv6, or UDPv6. If used with the –s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.

- -r Displays the routing table.
- -s Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
- interval Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

ROUTE - You can use the route command line tool to display the current IP routing table and add or delete IP routes.

ROUTE [-f] [-p] [command] [destination] [MASK netmask] [gateway] [METRIC metric] [IF interface]

- -f Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.
- -p When used with the ADD command, makes a route persistent across boots of the system. By default, routes are not preserved when the system is restarted. Ignored for all other commands, which always affect the appropriate persistent routes.

commands

- PRINT Prints a route
- ADD Adds a route
- DELETE Deletes a route
- CHANGE Modifies an existing route

- destination - Specifies the host.
- MASK -Specifies that the next parameter is the 'netmask' value.
- netmask - Specifies a subnet mask value for this route entry. If not specified, it defaults to 255.255.255.255.
- gateway - Specifies gateway.
- interface - Specifices the interface number for the specified route.
- METRIC - Specifies the metric, ie. cost for the destination.

All symbolic names used for destination are looked up in the network database file NETWORKS. The symbolic names for gateway are looked up in the host name database file HOSTS.

If the command is PRINT or DELETE. Destination or gateway can be a wildcard, (wildcard is specified as a star '*'), or the gateway argument may be omitted.

If Dest contains a * or ?, it is treated as a shell pattern, and only matching destination routes are printed. The '*' matches any string, and '?' matches any one char. Examples: 157.*.1, 157.*, 127.*, *224*.

Invalid MASK generates an error, that is when (DEST & MASK) != DEST.

Example> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1 The route addition failed: The specified mask parameter is invalid. (Destination & Mask) != Destination.

Examples:

route PRINT
route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
destination^ mask^ gateway^ metric^ ^Interface

If IF is not given, it tries to find the best interface for a given gateway.

route PRINT 112* .... Only prints those matching 112*
route CHANGE 112.0.0.0 MASK 255.0.0.0 112.89.8.5 METRIC 2 IF 2

CHANGE is used to modify gateway and/or metric only.

HOSTNAME - Hostname is used to show the local computer's host name for authentication by the Remote Copy Protocol (RCP), Remote Shell (RSH), and Remote Execution (REXEC) tools

TRACERT - Tracert is sometimes used to verify that IP addressing has been correctly configured on a client. It will basically show the route taken to reach a remote system

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:

- -d Do not resolve addresses to hostnames.
- -h maximum_hops Maximum number of hops to search for target.
- -j host-list Loose source route along host-list.
- -w timeout Wait timeout milliseconds for each reply.

PATHPING - Pathping also shows the route taken to reach a remote system as does TRACERT but PATHPING does so with more detail and allows for more functionality as well.

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n] [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T] [-4] [-6] target_name

Options:

- -g host-list Loose source route along host-list
- -h maximum_hops Maximum number of hops to search for target.
- -i address Use the specified source address.
- -n Do not resolve addresses to hostnames.
- -p period Wait period milliseconds between pings.
- -q num_queries Number of queries per hop.
- -w timeout Wait timeout milliseconds for each reply.
- -P Test for RSVP PATH connectivity.
- -R Test if each hop is RSVP aware.
- -T Test connectivity to each hop with Layer-2 priority tags.
- -4 Force using IPv4.
- -6 Force using IPv6.

There are additional tools that can be used to test TCP/IP connectivity. They are standard use tools for the TCP/IP protocol. **FTP**

- FTP is the File Transfer Protocol and it is used to transfer files from system to system.

Internet Explorer interconnectivity allows for a Windows Explorer type of GUI environment for the file transfer by allowing functionality of file and folder views and drag and drop / copy and paste.

The command line FTP allows for more functionality. FTP is considered to be a connected session using Transmission Control Protocol (TCP).

FTP commands are listed in the table below.

!	delete	literal	prompt	send
?	debug	ls	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recv	verbose
bye	hash	mls	remotehelp	
cd	help	mput	rename	
close	lcd	open	rmdir	

FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-w:windowsize] [-A] [host]

- -v Suppresses display of remote server responses.

- -n Suppresses auto-login upon initial connection.
- -i Turns off interactive prompting during multiple file transfers.
- -d Enables debugging.
- -g Disables filename globbing (see GLOB command).
- -s:filename - Specifies a text file containing FTP commands; the commands will automatically run after FTP starts.
- -a Use any local interface when binding data connection.
- -A - login as anonymous.
- -w:buffersize - Overrides the default transfer buffer size of 4096.
- host - Specifies the host name or IP address of the remote host to connect to.

[NOTES FROM THE FIELD] - *Use mget and mput commands take y/n/q for yes/no/quit.*
Use Control-C to abort actively executing commands.

TFTP - The Trivial File Transfer Protocol allows for the connectionless transfer of files to and from systems using User Datagram Protocol (UDP).

[NOTES FROM THE FIELD] - *User Datagram Protocol (UDP) is a connectionless protocol that does not guarantee delivery of data packets between hosts and is used when data transfer acknowledgments are not required. It can transmit only small portions of data at a time because it is not capable of segmenting and reassembling frames and does not implement sequence numbers.*

While TFTP is limited in functionality, there are still some command line switches that can be used to tailor its performance.

TFTP [-i] host [GET | PUT] source [destination]

- -i Specifies binary image transfer mode (also called octet). In binary image mode the file is moved literally, byte by byte. Use this mode when transferring binary files.
- host - Specifies the local or remote host.
- GET - Transfers the file destination on the remote host to the file source on the local host.
- PUT - Transfers the file source on the local host to the file destination on the remote host.
- source - Specifies the file to transfer.
- destination - Specifies where to transfer the file.

TELNET - Telnet is a terminal emulation program, which allows user to perform commands on a remote computer from a command window.

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]

- -a Attempt automatic logon. Same as -l option except uses the currently logged on user's name.
- -e Escape character to enter telnet client prompt.
- -f File name for client side logging
- -l Specifies the user name to log in with on the remote system. Requires that the remote system support the TELNET ENVIRON option.
- -t Specifies terminal type. Supported term types are vt100, vt52, ansi and vtnt only.
- host - Specifies the hostname or IP address of the remote computer to connect to.
- port - Specifies a port number or service name.

RCP - RCP copies files to and from computer running the RCP service. RCP uses the Transmission Control Protocol (TCP) to utilize the connected and reliable delivery of data between the client and the host and can be scripted in a batch file and does not require a password. The remote host must be running the RSHD service, and the user's username must be configured in the remote host's .rhosts file. RCP is one of the r-commands available on all UNIX systems.

[NOTES FROM THE FIELD] - *Microsoft's implementation of TCP/IP includes the RCP client software but not rshd services.*

RCP [-a | -b] [-h] [-r] [host][.user:]source [host][.user:] path\destination

- -a Specifies ASCII transfer mode. This mode converts the EOL characters to a carriage return for UNIX and a carriage return/line feed for personal computers. This is the default transfer mode.
- -b Specifies binary image transfer mode.
- -h Transfers hidden files.
- -r Copies the contents of all subdirectories; destination must be a directory.
- host Specifies the local or remote host. If host is specified as an IP address OR if host name contains dots, you must specify the user.
- .user: Specifies a user name to use, rather than the current user name.
- source Specifes the files to copy.
- path\destination Specifies the path relative to the logon directory on the remote host. Use the escape characters (\ , ", or ') in remote paths to use wildcard characters on the remote host.

RSH - RSH is a TCP/IP utility that enables clients to run commands directly on remote hosts running the RSH service without having to log on to the remote host. RSH is one of the UNIX r-commands that are available on all UNIX systems.

[NOTES FROM THE FIELD] - *Microsoft's implementation of TCP/IP includes the RSH client software but not the RSH service. If a user on a computer running in a Windows domain tries to use RSH to run a command on a remote UNIX server that is running the RSH daemon, the domain controller is required by the RSH client in order to resolve the username of the user.*

REXEC - REXEC runs commands on remote hosts running the REXEC service and authenticates the user name on the remote host before executing the specified command.

REXEC host [-l username] [-n] command

- host Specifies the remote host on which to run command.
- -l username Specifies the user name on the remote host.
- -n Redirects the input of REXEC to NULL.
- command Specifies the command to run.

FINGER - FINGER is a TCP/IP utility used for viewing information about a user on a system running the finger service.

Typing the command finger jason@windowsxp.2000trainers.com displays information about user Jason on a server called windowsxp.2000trainers.com.

FINGER [-l] [user]@host [...]

- -l Displays information in long list format.
- user Specifies the user you want information about. Omit the user parameter to display information about all users on the specified host.
- @host Specifies the server on the remote system whose users you want information about.

[NOTES FROM THE FIELD] - *Microsoft's implementation of TCP/IP includes the FINGER client software but not the FINGER service. You are able to run the FINGER client on a machine running a Windows operating system that is connected to the Internet in order to obtain results from a remote UNIX server running the FINGER daemon as a FINGER gateway.*

Practical # 5: Windows Xp Networking Practical Labs

Managing desktop setting & Control Panel (performance options)

Select windows classic theme.

1. Right-click on **Desktop**
2. Click **Properties**
3. Select **Windows Classic**
4. Click **Apply**

5. Click **OK**

Customize start menu items.

1. Right Click on **Taskbar**
2. Click **Properties**
3. Uncheck **Group similar taskbar buttons**
4. Click **Start Menu**
5. Click **Classic Start menu**
6. Click **Customize**

Check following Advance Start menu options:

7. Display Administrative Tools
8. Display Favorites
9. Display Log Off
10. Display Run
11. Enable dragging and dropping
12. Use Personalized Menus
13. Click **OK**
14. Click **Apply**
15. Click **OK**

Customize files, folders and windows.

1. Double-click My Computer
2. Select Icons
3. Tools
4. Folder Options
5. General Tab Select followings:
6. Use Windows classic folders
7. Open each folder in the same window
8. Double-click to open an item
9. View
10. Apply to All Folders
11. Apply
12. Ok

4- **Disable Windows Firewall, Automatic Updates and Change Security Center alerts for enable other PC's to ping i.e \\ping server.**

Start □
Settings □
Control Panel □
Double-click Security Center □
Windows Firewall □
Select Off (not recommended) □
Ok
Automatic Updates □
Select Turn off Automatic Updates □
Apply □
Ok
Resources:
Change the way Security Center Alerts me □
Uncheck following Alert Settings:
Firewall □
Automatic Updates □
Virus Protection □
Ok

Disable user switching and enable offline files.

You must have a computer administrator account on a computer that is a member of a workgroup or is a stand-alone computer to turn on or turn off the User Fast User Switching feature. Fast User Switching is not available on computers that are members of a network domain.

Start □
Settings □
Control Panel □
Double-click User Accounts □
Change the way users log on or off □
Uncheck following options from User Accounts:
Use the Welcome screen □
Use Fast User Switching □
Apply Options □

Offline Files overview

You can make network files available offline by storing shared files on your computer so they are accessible when you are not connected to the network.

This can be helpful when you use a portable computer to accomplish most of your work, or if your stand-alone computer is frequently disconnected from the network. You can work with offline files the same way you work with files when you're connected to the network.

When you reconnect to the network, any changes that you made to files while working offline are updated to the network. This process is called synchronization. If you and someone else on the network made changes to the same file, you can save your version of the file to the network, keep the other version, or save both.

If you share folders on your computer with others on the network, they can work offline with those folders. To protect files in your shared folders, you can specify whether other users can change your documents or just view them. You can also control which shared files users can access offline.

Enable offline files:

Double-click My Computer
Tools
Folder Options
Offline Files Tab
Check Enable Offline Files
Apply
Ok

6- **Sharing and Security settings.**

Double-click My Computer
Tools
Folder Options
View
Advance settings:
Uncheck use simple file sharing (Recommended)
Apply
Ok

7- **Assigning IP address and display network icon in notification area.**

Double-click My Network Places
Right-click
Properties
Right-click on Local Area Connection
Properties
Check following options from General Tab:
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
Select Internet Protocol (TCP/IP)
Properties
Select use the following IP Address:
IP address: 192.168.0.1
Subnet mask: 255.255.255.0
Ok

8- **Set up hardware profiles for different hardware configuration. At startup, you can choose the profile you want to use.**

Hardware profiles provide a way for you to set up and store different hardware configurations. You can set up hardware profiles for different hardware configurations. At startup, you can choose the profile you want to use.

Right-click on My Computer
Properties
Hardware Tab
Hardware Profiles
Select Profile 1 (Current) from Available hardware profiles:
Copy
Copy Profile name To: Home
Ok
Ok

9- **Select default operating system at system startup "Microsoft Windows XP Professional" or "Microsoft Windows Server 2003".**
Right-click on My Computer □
Properties □
Advance Tab □
Startup and Recovery:
Settings □
Select Default operating system □
Uncheck following from System startup:
Time to display list of operating systems: □
Time to display recovery options when needed: □
Ok □
Ok
10- **Delete old operating system support files (AUTOEXEC.BAT, CONFIG.SYS, IO.SYS, MSDOS.SYS).**
Double-click My Computer □
Tools □
Folder Options… □
View □
Select Show hidden files and folders □
Uncheck following from Advanced settings: □
Hide extensions for known file types
Hide protected operating system files (Recommended) □
Apply □
Ok
Goto C:\ and delete following files (these files are used for old operating system software)
AutoExec.bat
Config.sys
IO.sys
MSDOS.sys
11- **Enable/Disable hiberfil.sys (this file is use for hibernation i.e when we hibernate windows it keep all the open windows, files etc in hibernate file and when we start windows**
it shows all the files and windows in the same place.
When your computer hibernates, it stores whatever it has in memory on your hard disk and then shuts down. When your computer comes out of hibernation, it returns to its previous state.
Start □
Settings □
Control Panel □
Double-click Power Options □
Hibernate Tab □
Uncheck Enable Hibernation □
Apply □
Ok
12- **Remove pagefile.sys from C:\ drive or move it to any other drive. Pagefile.sys support RAM it is by default 1 and half of the RAM size.**
Right-click on My Computer □
Properties □
Advanced □
Select from Performance:
Settings □
Advance Tab □
Virtual memory:
Change □
Select C: from drive □
Custom size:
Initial size (MB): 0 □
Maximum size (MB): 0 □
Set □
Ok □
Apply □
Ok □
Ok

Restart computer to take effect.
Right-click on My Computer □
Properties □
Advanced □
Select from Performance:
Settings □
Advance Tab □
Virtual memory:
Change □
Select D: from drive □
Custom size:
Initial size (MB): 100 □
Maximum size (MB): 300 □
Set □
Ok □
Apply □
Ok □
Ok
Restart computer to take effect. After restart the file will more to drive D:\